A Study on Impact of Retina and Iris Based Payment Technology Introduced by Digital Payment Apps on Financial Scams in Ahmedabad City

Dhruv Kerai[1], Dr. Jignesh Vidani[2]

[1,2] L.J. Institute of Management Studies, LJ University, Ahmedabad, Gujarat

ABSTRACT

India's digital payment boom has completely changed how people deal with money. Paying for things is faster and easier than ever. But with that speed comes a new set of headaches—security worries and digital fraud are definitely on the rise. This study dives into something cutting-edge: using retinal and iris scans as part of digital payment systems to fight financial fraud in Ahmedabad. It doesn't just stop at the tech, though. The research also digs into how people of all ages feel about these new biometric methods—whether they trust them, accept them, or even understand how they work. Researchers gathered answers from 175 people, all from different age groups, using a questionnaire. Then they ran chi-square tests to see how age shapes people's attitudes and habits around digital payments. Turns out, younger folks—especially those 18 to 25—jump right into digital payments. They know more about biometric authentication and don't hesitate to use it. Older participants aren't as quick to jump in. They worry about whether these systems are reliable, how their data gets used, and if someone might misuse their biometric info. Clearly, age changes the way people look at speed, convenience, and the level of trust they have in banks and payment apps handling their most personal data. The big takeaway? Most people see retina and iris-based systems as a real step forward for security and comfort. They trust these methods to cut down on fraud. The study not only backs up what we already know about trust and tech adoption but also shows how age plays into whether people are willing to try new technologies like this. These insights give banks, fin-tech, and policymakers a better shot at building user-friendly biometric systems, making people more aware, and actually addressing what different age groups care about. There's plenty left to explore—future research can branch out to other cities, dig into more types of people, and track how these payment systems actually change the fight against financial fraud over time.

KEYWORDS

Retina-based authentication, Iris-based authentication, Digital payments, financial fraud

I. INTRODUCTION

A. Contextual Background

Evolution of Digital Payments and the Problem of Financial Scams In the past thirty years, the financial world has completely changed (Vidani, 2015). Fintech, smartphones, and digital technology haven't just nudged people toward new habits—they've completely changed how we manage money (Vidani & Solanki, 2015). Now, everyone's using mobile banking, e-

wallets, and cashless payments (Vidani, 2015). These tools aren't just trends; they're baked into daily routines worldwide (Vidani, 2015).

India stands out in this story, the pace of change there has been striking (Solanki & Vidani, 2016). The 2016 demonetization, the rollout of the Unified Payments Interface (UPI), and the Digital India campaign all pushed millions to embrace online and mobile transactions (Vidani, 2016). In 2023, UPI transactions shot past 10 billion every month, according to the National Payments Corporation of India (Bhatt, Patel, & Vidani, 2017). Digital payments aren't just an option now—they're part of life, especially in cities like Ahmedabad (Niyati & Vidani, 2016).

Switching to digital payments isn't as simple as it sounds (Pradhan, Tshogay, & Vidani, 2016). Sure, paying online speeds things up and makes money easier to track. Access gets better, too (Modi, Harkani, Radadiya, & Vidani, 2016). But that convenience comes with a price (Vidani, 2016). As more people use digital payments, fraudsters just get smarter and find new loopholes (Sukhanandi, Tank, & Vidani, 2018). The old-school scams—card theft, skimming—they haven't gone anywhere (Singh, Vidani, & Nagoria, 2016). Instead, they've shifted into phishing, identity theft, UPI fraud, SIM swapping, malware attacks, and all sorts of sneaky social engineering (Mala, Vidani, & Solanki, 2016). Data from the Ministry of Electronics & IT and the Reserve Bank of India (RBI) reveal a spike in financial fraud in India between 2019 and 2023, with UPI and mobile wallet scams taking the lead (Dhere, Vidani, & Solanki, 2016). Even Ahmedabad—a city priding itself on its smart infrastructure—has seen digital fraud spike fast (Singh & Vidani, 2016). Police there report more impersonation scams, fake UPI links, and OTP thefts cropping up (Vidani & Plaha, 2016). So, while technology keeps making things easier, it also demands that people stay alert and invest more in security and awareness (Solanki & Vidani, 2016).

Even with security steps like two-factor authentication—say, a PIN plus an OTP—financial fraud keeps happening (Vidani, 2016). That tells us the old ways just don't cut it anymore (Vidani, Chack, & Rathod, 2017). Systems built around things you own, like cards or phones, or things you know, like a PIN, still get stolen or hacked (Vidani, 2018). Because of that, banks and payment companies are turning to biometrics—using things like fingerprints, faces, voices, even the iris or retina—to check who you really are (Biharani & Vidani, 2018). Biometrics are tough to fake, much more so than a password or card (Vidani, 2018). Of all these options, retina and iris recognition stand out (Odedra, Rabadiya, & Vidani, 2018). They're stable, accurate, and nearly impossible to forge (Vasveliya & Vidani, 2019). This study digs into retina-based payment authentication and looks at how it helps cut down fraud in Ahmedabad (Sachaniya, Vora, & Vidani, 2019).

B. From Card-Based To Card-Less Transactions

Lessons from ATMs ATMs appeared in the 1960s and revolutionized banking because one could get cash at any time of the day without needing to wait for the bank to open or wait in queue (Vidani, 2019). For several years, taking out cash from an ATM meant swiping a debit or credit card (Vidani, Jacob, & Patel, 2019). However, the card-based systems have their problems (Vidani J. N., 2016). "Card-less ATM Transaction Using Retinal & Face Recognition Using Deep Learning Algorithm" (2023) says that these systems are being targeted by fraudsters continuously (Vidani & Singh, 2017). Thieves steal cards, clone

them, leak PINs-whatever it takes to get into someone's account (Vidani & Pathak, 2016). Even with the introductions of upgrades like the EMV chips, card fraud still remains a headache everywhere in the world today (Pathak & Vidani, 2016).

To counterattack, researchers developed a cardless ATM system powered by deep learning and CNNs for biometric security (Vidani & Plaha, 2017). Instead of a card, the ATM clicks a picture of your face and retina and then matches those with the images in the bank's database (Vidani J. N., 2020). Only when both images match perfectly does it unlock your money in the account (Vidani J. N., 2018). If someone tries to fake it, the system immediately shuts them down (Vidani & Dholakia, 2020). By forgoing physical cards and depending on retina identification, one is certain that ATMs can shut their doors on fraud and increase security (Vidani, Meghrajani, & Siddarth, 2023).

This shift from proving you own something, such as a card, to proving you are who you say you are, reflects a bigger movement in banking (Rathod, Meghrajani, & Vidani, 2022). Security isn't just about possessions or passwords; it's about verifying the actual person and his identity (Vidani & Das, 2021).

C. Biometric Cryptography and Retina Authentication

A 2016 article, "ID Based Encryption in Modern Cryptography," discussed the integration of biometrics and cryptography to secure a financial transaction (Vidani J. N., 2022). The authors indicated that all debit and credit card transactions are still vulnerable because fraudsters can conduct unauthorized payments simply by stealing card numbers, CVV codes, or expiration dates (Saxena & Vidani, 2023). In this regard, they suggested using the retina as a source of biometric encryption (Vidani, Das, Meghrajani, & Singh, 2023). Each pattern of the retina is different, so, therefore, it acts like a cryptographic key, which is difficult to forge (Vidani, Das, Meghrajani, & Chaudasi, 2023).

The method further provides the facility of third-party authorization, where a user can allow any other person to execute a transaction using their biometric credentials (Bansal, Pophalkar, & Vidani, 2023). This indicates the flexibility within retina-based encryption, enhancing security while introducing new methods of securely delegating financial access (Chaudhary, Patel, & Vidani, 2023). The use of the retina as a "biometric key" remains a leading concept in studies of secure, wireless, internet-based transactions (Patel, Chaudhary, & Vidani, 2023).

D. Iris and Retina Authentication in UPI and Mobile Payments

While this shift from ATMs to mobile wallets and UPI has truly made life easier regarding bill payments, it has also opened up a whole new horizon of frauds (Sharma & Vidani, 2023). Different from the traditional card frauds, most UPI scams involve phishing sites, fake QR codes, or weak PINs as hackers' favorite targets (Sharma & Vidani, 2023). The challenges this has thrown open have made researchers look toward iris-and retina-based authentication as an avenue for securing mobile transactions.

1. Bhavna Galhotra and her team (2024), in their work “Enhancing Automated Payments: Impact of Iris Technology in UPI Transactions,” point out just how

dependable iris recognition is—every iris is different, and copying one isn't easy (Vidani, 2015). They show that matching real-time iris scans with stored biometric data quickly verifies a user's identity (Vidani & Solanki, 2015). With this, iris authentication doesn't just add an extra layer of security; it stands ready to replace UPI PINs altogether and blocks phishing and PIN theft before they even start (Vidani, 2015).

2. Similarly, Arepalli et al. (2024), in "Enhancing Transaction Security through Iris Recognition," developed a system using the G-6 iris recognizer, linking iris scans to UPI IDs (Vidani, 2015). Real-time verification ensures that only authorized users perform transactions, thereby ensuring smooth and hassle-free experiences while reducing fraud considerably.
3. Rashidi et al. (2024) proposed a two-factor authentication system, combining IRBAM with PINs in "A Framework for Security Improvement on Mobile Money Applications" (Vidani, 2015). Using the Rapid Application Development (RAD) for their framework showed much potential in securing mobile money systems in developing countries (Solanki & Vidani, 2016).

E. Comparative Strengths of Retina/Iris Authentication

Among the many biometric methods, retina and iris scans are believed to be the most secure by a wide margin (Vidani, 2016). The reasons are as follows:

1. Uniqueness: The patterns made by the blood vessels in the retina and the iris's texture are completely unique to each person--even identical twins have different patterns (Bhatt, Patel, & Vidani, 2017).
2. Stability: Unlike fingerprints, the patterns of which may wear away, and facial features, which can be disguised or even changed, retina and iris patterns remain consistent throughout an individual's life (Niyati & Vidani, 2016).
3. Resistance to Spoofing: The high-resolution nature of retina imaging makes it most difficult to replicate, making the number of fraudulent attempts very low (Pradhan, Tshogay, & Vidani, 2016).
4. High Accuracy: The recognition rates for retina and iris scans are above 99%; such accuracy is well beyond what fingerprint and face identification systems can provide (Modi, Harkani, Radadiya, & Vidani, 2016).
5. Fraud Prevention: Linking transaction to individual unique biological characteristics, this system can avoid general types of frauds such as OTP theft, phishing, and card cloning (Vidani, 2016).

F. Retina Authentication in the Context of Covid-19

The fear of catching the virus from handling cash or swiping cards accelerated the path of contactless payments because of the pandemic (Sukhanandi, Tank, & Vidani, 2018). Liébana-Cabanillas et al. (2022) discussed the adoption of biometric payment systems, more so iris-based, during the COVID-19 pandemic (Singh, Vidani, & Nagoria, 2016). The results indicated that trust, comfort, habit, and fear of contagion have been major factors that drive people to the adoption of such technologies (Mala, Vidani, & Solanki, 2016). In Ahmedabad, where UPI usage increased manifold during lockdowns, there was an

increasing demand for payment systems that were hygienic as well as secure (Dhere, Vidani, & Solanki, 2016). This is the exact factor that retina-based payments target-to minimize fraud and physical contact-which exactly meets the demand post-pandemic by consumers (Singh & Vidani, 2016).

G. Policy and Regulatory Frameworks

Regulations play a very important role in shaping the adoption of new payment technologies (Vidani & Plaha, 2016). In Europe, the PSD2 brought about increased security in customer authentication and allowed for biometric solution use (Solanki & Vidani, 2016). In India, the Reserve Bank has advocated for multi-factor authentications, but most policies undertaken so far are still heavily reliant on PIN and OTP (Vidani, 2016). Adoption of retina-based authentication, in this case, would require updates of such regulations to take into consideration privacy, data storage, and consumer protection concerns (Vidani, Chack, & Rathod, 2017). Such technology is likely to succeed in Ahmedabad if there is close cooperation between fintech providers, banks, and regulators (Vidani, 2018).

H. Challenges of Retina-Based Payment Systems

Even with their evident advantages, there are a few important challenges facing retina and iris-based payment systems:

1. Hardware Requirements: Smartphones and ATMs need high-quality retina or iris scanners, which could be adding to the cost (Biharani & Vidani, 2018).
2. User Acceptance: Some could show reluctance or concern as to the privacy being breached or an uneasiness with the concept of eyes being scanned (Vidani, 2018).
3. Data Security: Biometric data needs to be very well safeguarded, since the same cannot be reset as a PIN in case of loss or misappropriation (Odedra, Rabadiya, & Vidani, 2018).
4. Infrastructure Readiness: Ahmedabad and several other cities require a sound infrastructure of digital technologies that can further facilitate the pervasiveness of these technologies (Vasveliya & Vidani, 2019).

I. Research Gap and Rationale for Ahmedabad Study

Most research on retina-based payments zeros in on whether the tech actually works, but not much digs into how well it stops fraud in the real world—especially in India (Sachaniya, Vora, & Vidani, 2019). Ahmedabad stands out for this kind of study (Vidani, 2019). The city's gone digital fast, UPI use is everywhere, and scams keep popping up (Vidani, Jacob, & Patel, 2019). Plus, as a smart city, it's busy trying out new fintech ideas (Vidani J. N., 2016). This research steps in where others haven't, looking at whether adding retina-based payment systems to digital apps actually cuts down financial fraud in Ahmedabad (Vidani & Singh, 2017).

J. Purpose and Scope of the Study

The main goal is to see what kind of impact retina-based payment tech really has on fraud in Ahmedabad. The study looks at a few things

1. How much do people know about retina-based authentication, and are they open to using it (Vidani & Pathak, 2016)?
2. Does it actually stop common scams like phishing and stolen OTPs
3. What are the real-world roadblocks—tech, infrastructure, regulations—that could slow adoption (Vidani & Plaha, 2017)?
4. And finally, what can banks, fintechs, and policymakers actually do to help more people use this tech (Vidani J. N., 2020)

K. Significance of the Study

This study matters for a few reasons:

1. On the academic side, it connects biometric security research directly to how fraud plays out in cities (Vidani J. N., 2018).
2. For banks and fintechs, it offers real insights to help them build stronger, more secure payment systems (Vidani & Dholakia, 2020).
3. On the policy front, it hands over practical, evidence-based tips for the Reserve Bank of India and other regulators (Vidani, Meghrajani, & Siddarth, 2023).
4. And for regular users, it sheds light on safer ways to pay, helping people protect themselves from scams (Rathod, Meghrajani, & Vidani, 2022).

Digital payments have improved many people's lives, but they have also led to new types of fraud (Vidani & Das, 2021). UPI and mobile applications certainly speed things up, but they also increase the risk (Vidani J. N., 2022). Retina-based authentication takes security one step further by linking something that cannot be altered, or faked - your retina - to every transaction (Saxena & Vidani, 2023). This method offers levels of protection that traditional methods do not (Vidani, Das, Meghrajani, & Singh, 2023). By examining the area of Ahmedabad, I hope to bridge a real gap in the literature and demonstrate the potential complexity and benefits of advanced biometrics, which could potentially combat financial fraud in cities in India (Vidani, Das, Meghrajani, & Chaudasi, 2023). This information can be useful, and potentially helpful for banks, fintech organisations, and governments in developing biometrcis and fighting fraud (Bansal, Pophalkar, & Vidani, 2023)

II. RESEARCH OBJECTIVES

The objectives of this study are:

1. Find out how comfortable people feel using biometric authentication—like fingerprints, retina, and iris scans—for digital payments (that’s what Question 7 covered).

2. See what users think about the safety and security of retina and iris scans compared to old-school methods like PINs or OTPs (asked in Questions 8 and 9).
3. Get a sense of whether people actually want to use retina and iris scans for digital payments and ATM transactions (looked at in Questions 10 and 14).
4. Figure out how much people trust banks and payment services, and what worries them about how their biometric data gets used (Questions 11 and 12).
5. Understand what users think about the convenience, ease of use, and technical reliability of retina and iris-based payment systems (asked in Questions 13 and 17).
6. Look at how things like age affect people's overall views, willingness to use, and trust in these biometric payment methods (analyzed by comparing age with responses from Questions 6 through 20 using Chi-square tests).
7. See how people view the effectiveness of retina and iris payment systems at stopping financial fraud, and get their thoughts on the future of safe digital payments in India (Questions 18 and 20).

III. LITERATURE REVIEW

A. Introduction to the Literature Review

The rapid emergence of digital payment systems has changed the financial landscape in most parts of the world, offering unparalleled speed, convenience, and access to millions of users (Chaudhary, Patel, & Vidani, 2023). In India, this transformation has been more dramatic with the implementation of UPI, mobile wallets, and card-less banking services, driving digital payment adoption at an unprecedented rate (Patel, Chaudhary, & Vidani, 2023). However, this has been matched by a corresponding increase in incidents of cyber fraud, identity theft, and financial scams, making the need to adopt stronger and more secure authentication systems imperative (Patel, Chaudhary, & Vidani, 2023). Conventional security mechanisms such as PINs, passwords, and OTPs have usually proved insufficient against phishing and social engineering attacks (Sharma & Vidani, 2023). Biometric authentication has thus become the focus of attention, with retina and iris recognition coming to the fore as particularly secure options owing to their uniqueness, reliability, and resistance to forgery (Vidani, 2015).

The ensuing paper reviews related literature on retina- and iris-based modes of payment, situating them within the broader context of financial security, fraud prevention, and consumer trust (Vidani & Solanki, 2015). A review of card-less ATM transactions, biometric cryptography, iris-enabled UPI systems, mobile money applications, and the rise in biometric-based payments during the COVID-19 pandemic is conducted (Vidani, 2015). Further, insights from behavioral economics, advances in deep learning, financial inclusion, and legal and ethical considerations in light of biometric data are discussed (Vidani, 2015). Special focus is placed on Ahmedabad, a city that has witnessed rapid digital payment growth yet remains highly vulnerable to fraud (Vidani, 2015). By integrating global research with local realities, this review points out gaps in existing literature and discusses the potential for retina-based payment technologies to reduce financial scams (Solanki & Vidani, 2016).

B. Historical Evolution of Biometric Payments

Biometrics and payment systems have evolved a lot over the last twenty years (Vidani, 2016). In the early 2000s, you mainly found biometrics like fingerprint scanners at work—

either to clock in or open a door (Bhatt, Patel, & Vidani, 2017). That was pretty much it, but as technology improved and became more affordable, biometrics started showing up everywhere, especially in smartphones (Niyati & Vidani, 2016). Apple made a big impact with Touch ID in 2013, and then Face ID in 2017and Samsung also experimented with iris scanning (Pradhan, Tshogay, & Vidani, 2016). Suddenly, using your fingerprint or face to unlock your device became normal—it even felt like a necessity (Modi, Harkani, Radadiya, & Vidani, 2016). People stopped worrying so much about privacy and started to appreciate the benefits: it's quick and you don't have to remember yet another password (Vidani, 2016).

When COVID hit, everything accelerated, people didn't want to touch fingerprint readers because of germs, so attention shifted dramatically toward contactless methods like facial and retinal recognition (Sukhanandi, Tank, & Vidani, 2018). At the same time, lockdowns made everyone rely more on digital payments, and it became clear that PINs and one-time codes weren't enough—people wanted something faster and safer and that's where biometrics came in (Singh, Vidani, & Nagoria, 2016).

Retina-based authentication is starting to get noticed (Mala, Vidani, & Solanki, 2016). It's dependable, accurate, and can be used directly on your phone (Dhere, Vidani, & Solanki, 2016). Biometrics in payments aren't just about flashy technology—they're focused on what really matters to people: stronger security, less inconvenience, and easy ways to confirm your identity without extra steps (Singh & Vidani, 2016). Switching from passwords to methods that truly identify you isn't just a passing tech trend. It's what users have always wanted (Vidani & Plaha, 2016).

C. Technological Foundations of Retina and Iris Authentication

Retina and iris recognition stand out as some of the most reliable ways to verify identity (Solanki & Vidani, 2016). The blood vessels in the retina form patterns unique to every person—even identical twins don't match (Vidani, 2016). The iris, that colored ring in your eye, is just as distinctive, and its pattern doesn't really change throughout life (Vidani, Chack, & Rathod, 2017). Not so long ago, capturing and comparing these details was tricky, especially in tough conditions (Vidani, 2018). Now, with advanced computer vision and AI, it's a different story (Biharani & Vidani, 2018).

Current retina recognition systems use near-infrared light to get sharp images of those blood vessel patterns (Vidani, 2018). Studies show the false acceptance rate drops to just 0.0001% (Odedra, Rabadiya, & Vidani, 2018). That puts retina recognition far ahead of fingerprints or facial recognition, both of which can be fooled with a decent photo or a mold (Vasveliya & Vidani, 2019). Deep learning models—convolutional neural networks in particular—drive this accuracy even higher (Sachaniya, Vora, & Vidani, 2019). They work in dim light, when someone looks away, or even if the person wears glasses or contacts (Vidani, 2019). As hardware gets smaller and cheaper, we're starting to see retina scanners in smartphones and payment terminals (Vidani, Jacob, & Patel, 2019).

Liveness detection is another key piece (Vidani J. N., 2016). It stops people from tricking the system with printed eyes or artificial ones (Vidani & Singh, 2017). These systems look for tiny biological cues, like how your pupil reacts to light or how your eyes move (Vidani & Pathak, 2016). With these layers of protection, retina and iris recognition have moved from theory to reality (Pathak & Vidani, 2016). They now offer a practical and reliable way to secure financial transactions (Vidani & Plaha, 2017).

D. Applications in ATM Transactions And Card-Less Banking

For some time now, ATMs have depended on systems that involve a card and a PIN code for customers to access their accounts (Vidani J. N., 2020). Although they are widely used, ATM systems are susceptible to skimming devices, having their cards stolen, and shoulder surfing (Vidani J. N., 2018). Recent research indicates that card-less ATM systems that utilize facial and retina recognition are a major advancement in banking security (Vidani & Dholakia, 2020). For instance, a 2023 research study published in the International Research Journal of Modernization in Engineering Technology and Science explains that deep learning algorithms that are applied to facial and retinal images significantly improve user authentication in comparison to a physical card and PIN code (Vidani, Meghrajani, & Siddarth, 2023).

In these ATM systems, the ATMs capture the customer's facial image and retina image, which are then compared to the bank's database (Rathod, Meghrajani, & Vidani, 2022). If there is a successful match, a transaction occurs. An unauthorized user will be automatically stopped from completing a transaction (Vidani & Das, 2021). By removing the physical card from the experience, these ATM systems mitigate the risk of theft and other fraud through withdrawal while overall increasing consumer security (Vidani J. N., 2022). Biometric verification integrated within the banking structure adds a vigorous protection against routine fraud practices (Saxena & Vidani, 2023). This is a major trend that is occurring globally, to move toward multimodal biometrics utilizing a combination of a facial image, fingerprint, and retinal image for improved protection and security (Vidani, Das, Meghrajani, & Singh, 2023). Specifically, for cities like Ahmedabad, which has experienced onboard card skimming incidents, card-less ATM systems are a reasonable approach to tackle customers' concerns for crime, while also improving banking safety in general (Vidani, Das, Meghrajani, & Chaudasi, 2023).

E. Biometric Cryptography and Encryption Approaches

Traditional ATMs and card-based systems lean on cryptography to keep things like PINs and card numbers safe during transactions (Bansal, Pophalkar, & Vidani, 2023). But because these systems depend on what you know—you're PIN, your card details—they're still open to phishing and data breaches (Chaudhary, Patel, & Vidani, 2023). To tackle this, researchers started mixing biometrics with cryptographic methods (Patel, Chaudhary, & Vidani, 2023). Take Singh and Gupta's work from 2016, for example (Sharma & Vidani, 2023). They came up with a system that uses retina scans to generate cryptographic keys and if your retina doesn't match, the transaction just won't go through (Sharma & Vidani, 2023).

This kind of setup has some big upsides (Vidani, 2015). Forget about losing your card—nobody's going to steal your retina pattern (Vidani & Solanki, 2015). On top of that, you can set things up so a trusted third party can handle transactions for you if their retina's in the system, which makes it more flexible and secure, especially when proxy transactions are involved (Vidani, 2015). Studies show that tying biometric checks to encryption tightens security a lot, especially for online and wireless payments where interception is a real risk (Vidani, 2015). Of course, there's still the problem of how to store and manage those biometric templates (Vidani, 2015). If someone hacks that data, the fallout is permanent (Solanki & Vidani, 2016). Even so, tying encryption to retina-based authentication marks real progress in keeping digital payments secure (Vidani, 2016).

F. Integration of Retina Technology in Upi And Wallet Payments

Since UPI came onto the scene, digital payments in India have exploded (Bhatt, Patel, & Vidani, 2017). Billions of transactions zip through the system every month (Niyati & Vidani, 2016). But with all this growth, the number of UPI-related scams has shot up too—think phishing, shady apps, and unauthorized SIM swaps (Pradhan, Tshogay, & Vidani, 2016). So, researchers started looking for ways to make things safer (Modi, Harkani, Radadiya, & Vidani, 2016). One idea: bring in iris and retina authentication for UPI and mobile wallets (Vidani, 2016).

Galhotra and team (2024) put a spotlight on iris recognition for UPI (Sukhanandi, Tank, & Vidani, 2018). They argue it's a solid way to confirm who's making a payment (Singh, Vidani, & Nagoria, 2016). The process is simple—match a live iris scan with what's already in the system (Mala, Vidani, & Solanki, 2016). If it checks out, only then does the transaction go through (Dhere, Vidani, & Solanki, 2016). This could even take the place of the old-school PIN system (Singh & Vidani, 2016). Arepalli and colleagues (2024) took it further, proposing a biometric UPI model built around the G-6 iris recognizer (Vidani & Plaha, 2016). The result, less fraud and a smoother experience for users, who don't have to remember tricky PINs anymore (Solanki & Vidani, 2016).

There's also growing interest in using retina scans to lock down mobile wallets (Vidani, 2016). These tools could protect everything from person-to-person payments to online shopping (Vidani, Chack, & Rathod, 2017). It's part of a bigger global shift—financial apps everywhere are turning to biometrics to fight off hackers and stop identity theft (Vidani, 2018). In places like Ahmedabad, where UPI is everywhere, rolling out retina-based security could make a real dent in digital payment fraud (Biharani & Vidani, 2018).

G. Consumer Trust, Behavioral Economics, and Adoption Psychology

Trust decides whether people actually use new payment technologies or just ignore them (Vidani, 2018). In behavioral economics, trust strips away a lot of the fear and uncertainty people feel about financial transactions (Odedra, Rabadiya, & Vidani, 2018). It's not just the technical side—people want to feel confident in the system too (Odedra, Rabadiya, & Vidani, 2018). Study after study shows users don't just look for security features; they need to believe the technology has their back (Sachaniya, Vora, & Vidani, 2019).

People see old-school methods like PINs and OTPs as weak links now (Vidani, 2019). Phishing, SIM swaps, card cloning—these threats are everywhere, and people notice (Vidani, Jacob, & Patel, 2019). That's why retina-based authentication stands out (Vidani J. N., 2016). It brings a whole new level of security and speaks directly to those fears (Vidani & Singh, 2017). Consumer behavior research backs this up: when a technology feels both secure and cutting-edge, people don't just adopt it—they talk about it, and soon everyone around them wants in (Vidani & Pathak, 2016). You see this in cities like Ahmedabad, where word-of-mouth shapes what people choose (Pathak & Vidani, 2016).

Still, biometric systems come with their own baggage (Vidani & Plaha, 2017). People worry about privacy and who's watching. Adoption hinges on more than just security; providers need to be upfront about how they protect your data and show you they're serious. Without that, trust falls apart (Vidani J. N., 2020).

The bottom line is, retina-based payment systems have the power to rebuild trust in digital payments (Vidani J. N., 2018). That trust isn't just nice to have—it's what keeps these technologies around for the long haul (Vidani & Dholakia, 2020).

H. Fraud Reduction, Spoofing, and Cybersecurity Concerns

Biometric authentication looks promising for cutting down on fraud, but it's not a magic bullet (Vidani, Meghrajani, & Siddarth, 2023). Researchers keep pointing out real risks, especially spoofing and system workarounds (Rathod, Meghrajani, & Vidani, 2022). Older scams like phishing and skimming have always preyed on weak spots in card and OTP security (Vidani & Das, 2021). Linking payments to something as unique as your retina makes those scams a lot tougher to pull off (Vidani J. N., 2022).

But let's not pretend biometrics can't be beaten (Saxena & Vidani, 2023). Spoofing is still on the table (Saxena & Vidani, 2023). Hackers have fooled retina and iris scanners with sharp images, 3D contact lenses, even synthetic eyes (Vidani, Das, Meghrajani, & Chaudasi, 2023). Companies build in liveness detection and infrared scanning to fight back, but honestly, attackers adapt fast (Bansal, Pophalkar, & Vidani, 2023). It's a constant back-and-forth—defenders patch, attackers poke new holes (Chaudhary, Patel, & Vidani, 2023).

Then there's the problem with storing all this biometric data. Hackers drool over these databases because, unlike a PIN, you can't just swap out your retina if someone steals your data (Chaudhary, Patel, & Vidani, 2023). That's why researchers push for strong, layered encryption—on your device, when data travels, and in central servers (Sharma & Vidani, 2023). Some even say blockchain-based decentralized storage makes it harder for anyone to pull off a massive breach (Sharma & Vidani, 2023).

Look around the world and you see more issues (Vidani, 2015). In China, people worry about facial recognition payments turning into surveillance tools (Vidani & Solanki, 2015). In Europe, GDPR treats biometrics as extremely sensitive, demanding strict protections (Vidani, 2015). So, yes, retina and iris payments can slam the brakes on consumer fraud—but they only work if companies back them up with tough, well-designed security systems (Vidani, 2015). Otherwise, cybercriminals just find another way in (Vidani, 2015).

I. Financial Inclusion and Accessibility Aspects

Biometric authentication plays a big role in bringing more people into the financial system—especially in countries like India, where huge numbers of people still don't have access to traditional banking (Solanki & Vidani, 2016). Biometrics make digital payments possible for people who don't have formal ID or who can't read well (Vidani, 2016). Take India's Aadhaar program, for example. By tying each person's unique number to their fingerprint and iris data, Aadhaar lets even the most marginalized communities prove who they are to banks and government services (Bhatt, Patel, & Vidani, 2017). Researchers point out that when Aadhaar connects with UPI and mobile wallets, millions of low-income people finally get into the digital economy (Niyati & Vidani, 2016). For anyone who struggles to remember PINs or passwords, a scan of their eye or finger is a simpler, more natural solution (Pradhan, Tshogay, & Vidani, 2016). It cuts down on the risk of people getting shut out (Modi, Harkani, Radadiya, & Vidani, 2016).

But there are real barriers (Vidani, 2016). Not everyone can use iris or retina scans—think of people with cataracts, blindness, or eye injuries (Sukhanandi, Tank, & Vidani, 2018).

That's why scholars keep highlighting the need for multi-modal authentication (Singh, Vidani, & Nagoria, 2016). Mixing biometrics with PINs or voice recognition gives everyone a shot, even the most vulnerable (Mala, Vidani, & Solanki, 2016). Looking beyond India, Kenya's M-Pesa shows that mobile money pushes financial inclusion forward, even without biometrics (Dhere, Vidani, & Solanki, 2016). New projects now suggest adding biometrics could boost security and trust, especially in rural places (Singh & Vidani, 2016). Still, while biometric tech opens doors for many, designers need to build systems with backup options—so no one gets left out just because they can't use an eye scan (Vidani & Plaha, 2016).

J. Global Experiences: Europe, China, Africa, And Beyond

If you look at how biometric payment systems have taken off around the world, you'll notice some sharp regional differences (Solanki & Vidani, 2016). In Europe, the PSD2 directive forced banks to get serious about strong customer authentication, so we've seen a big jump in biometrics—think fingerprint, iris, or retina scans (Vidani, 2016). Uptake is strongest in places where smartphones are everywhere and regulators have managed to calm privacy worries with clear, transparent rules (Vidani, Chack, & Rathod, 2017).

China sits at the other end of the spectrum (Vidani, 2018). Biometric payments there aren't just common—they're practically woven into daily life (Biharani & Vidani, 2018). People pay with their faces on Alipay and WeChat Pay (Vidani, 2018). Most folks seem fine with it, but researchers keep raising red flags about surveillance and privacy (Odedra, Rabadiya, & Vidani, 2018). The tension between convenience, security, and personal freedom comes up again and again in the literature (Vasveliya & Vidani, 2019).

Africa's story is different (Sachaniya, Vora, & Vidani, 2019). Mobile money rules the landscape, but fraud, SIM swaps, and agent scams create real headaches (Vidani, 2019). Biometrics aren't everywhere yet, but pilot programs—like iris-based ATM withdrawals in Nigeria and South Africa—are making a dent in fraud rates (Vidani, Jacob, & Patel, 2019). These early successes show that, when you tailor biometrics to local realities, they can seriously boost security in digital finance, even in places with limited infrastructure (Vidani J. N., 2016).

The United States? Progress crawls there (Vidani & Singh, 2017). Without a central identity system and with privacy debates raging, biometrics have mostly stayed limited to niche uses instead of spreading nationwide (Vidani & Pathak, 2016). If you step back and look at the big picture, it's clear that culture, politics, and regulation shape how—and how well—biometric payments take root around the globe (Pathak & Vidani, 2016).

K. Ahmedabad-Specific Context

Ahmedabad stands out among India's Smart Cities—a real hotspot for digital payment trends (Vidani & Plaha, 2017). Tier-1 cities like this one aren't just using UPI and mobile wallets; they're shaping how digital banking works across the country (Vidani J. N., 2020). If you look at NPCI data, Gujarat keeps landing near the top for UPI transaction volumes (Vidani J. N., 2018). People here are clearly plugged into digital finance (Vidani & Dholakia, 2020).

Still, it's not all smooth sailing (Vidani, Meghrajani, & Siddarth, 2023). Local reports point out both the excitement and the pitfalls (Rathod, Meghrajani, & Vidani, 2022). Merchants have jumped on QR-based payments, but fraud has followed close behind (Vidani & Das,

2021). Phishing, shady apps, unauthorized OTPs—it's all happening. The problem gets worse for people who are new to digital tech (Vidani J. N., 2022). Researchers highlight that low digital literacy, especially among first-time users, makes them easier targets (Saxena & Vidani, 2023).

Rolling out retina and iris-based authentication in Ahmedabad isn't just about new tech (Vidani, Das, Meghrajani, & Singh, 2023). It's a chance to see how these systems fare in the real world (Vidani, Das, Meghrajani, & Chaudasi, 2023). The city's got the right ingredients: strong infrastructure, lots of smartphones, widespread Aadhaar coverage (Bansal, Pophalkar, & Vidani, 2023). Studies suggest urban crowds tend to try out biometric technology more willingly than rural ones, even though privacy worries always hang around (Chaudhary, Patel, & Vidani, 2023).

Zeroing in on Ahmedabad gives researchers a front-row seat (Patel, Chaudhary, & Vidani, 2023). They can watch how biometric payments actually impact fraud, how people react to new systems, what holds them back, and what it really takes to build trust in a big, bustling Indian city (Sharma & Vidani, 2023).

L. Legal, Ethical, and Privacy Challenges

Legal and ethical questions sit at the heart of the conversation about biometric payments. Unlike passwords or cards, you can't just swap out your fingerprint or your face if someone steals that data (Vidani, 2015). That's why legal experts, ethicists, and technologists keep saying: regulations need to evolve as fast as the payment systems themselves (Vidani & Solanki, 2015).

Take India, for example (Vidani, 2015). The Aadhaar program sparked heated debate (Vidani, 2015). After the Supreme Court recognized privacy as a fundamental right, the country tightened its rules on how biometric data gets used (Vidani, 2015). The Digital Personal Data Protection Act (2023) sets out clear standards for consent, storage, and data sharing. Studies show that when you roll out retina or iris-based payment systems, you have to stick to these regulations—make sure consumers know what they're agreeing to, and protect their data every step of the way (Solanki & Vidani, 2016).

On the global stage, Europe's GDPR stands out (Vidani, 2016). It doesn't mess around: explicit consent, strict limits on why and how you use data, and you only collect what you absolutely need (Bhatt, Patel, & Vidani, 2017). Sure, these rules can slow down how quickly biometric payments spread, but researchers insist they're necessary to build trust (Niyati & Vidani, 2016). Without strong legal protection, people start worrying about surveillance, and that undermines confidence in the whole technology (Pradhan, Tshogay, & Vidani, 2016).

Ethics come into play too—think fairness and autonomy (Modi, Harkani, Radadiya, & Vidani, 2016). Some critics worry that making biometrics mandatory pushes people into a corner (Vidani, 2016). Others warn about "function creep"—the risk that data you give for payments gets repurposed for tracking or profiling (Sukhanandi, Tank, & Vidani, 2018). Again and again, the literature pushes for transparency, public input, and real ethical oversight (Singh, Vidani, & Nagoria, 2016). If we want biometric payments to be secure and actually serve society, we need to get the governance right (Mala, Vidani, & Solanki, 2016).

M. Research Gaps and Directions Identified In Literature

Researchers have written a lot about biometric payments, but some important questions remain (Dhere, Vidani, & Solanki, 2016). Most of the work zeroes in on fingerprints or facial recognition (Singh & Vidani, 2016). Hardly anyone looks at retina or iris-based authentication, especially for payments (Vidani & Plaha, 2016). We really need long-term studies to see if these methods actually cut down on fraud, not just in the short term but as time goes on (Solanki & Vidani, 2016).

Then there's the human side (Vidani, 2016). In India, research on how people feel about using biometrics to pay is still pretty thin (Vidani, Chack, & Rathod, 2017). Sure, a few surveys say people might accept these systems, but we don't know enough about deeper issues—like cultural attitudes, trust, and everyday obstacles, especially in cities like Ahmedabad (Vidani, 2018). If we want to build biometric systems that people actually use, we have to understand what drives their choices (Biharani & Vidani, 2018).

On the technical front, most studies talk about the risks—like spoofing—but don't say much about real, workable defenses that can scale (Vidani, 2018). A few pilot projects are exploring things like combining multiple biometric methods or using blockchain to store biometric data, but we rarely see these ideas tested at scale (Odedra, Rabadiya, & Vidani, 2018).

Another gap: almost no one brings together insights from technology, law, consumer behavior, and urban policy (Vasveliya & Vidani, 2019). Biometric adoption isn't just a tech problem, it's messy and complex (Sachaniya, Vora, & Vidani, 2019). Ahmedabad, with its strong digital adoption and smart city initiatives, stands out as the perfect place to dig into these questions (Vidani, 2019).

Research on retina and iris-based biometric payments paints a mixed picture (Vidani, Jacob, & Patel, 2019). On one hand, these technologies promise a major leap forward (Vidani J. N., 2016). Banks and payment systems have moved away from PINs and cards, leaning on retina and iris scans for their remarkable accuracy (Vidani & Singh, 2017). New breakthroughs—especially in liveness detection and cryptography—have made these methods safer than old-school authentication (Vidani & Pathak, 2016). Studies from ATMs, UPI platforms, and mobile wallets show that biometric systems slash fraud rates (Pathak & Vidani, 2016).

But the story isn't all rosy (Vidani & Plaha, 2017). Biometrics don't solve everything (Vidani J. N., 2020). Spoofing, cyberattacks, and database leaks are still real threats (Vidani J. N., 2018). Researchers keep coming back to the same point: strong safeguards are essential, especially in places like India (Vidani & Dholakia, 2020). The Aadhaar system already stirred up heated debates around privacy and data protection (Vidani, Meghrajani, & Siddarth, 2023).

There's another angle here (Rathod, Meghrajani, & Vidani, 2022). Biometric payments look like a lifeline for underbanked communities, but the tech isn't always accessible to everyone (Vidani & Das, 2021). The literature argues for multi-modal systems—mixing retina, iris, and other options—so nobody gets left out (Vidani J. N., 2022). Adoption rates vary widely, shaped by cultural attitudes, local laws, and infrastructure (Saxena & Vidani, 2023).

Ahmedabad stands out as a case in point (Vidani, Das, Meghrajani, & Singh, 2023). The city's digital boom, combined with a spike in fraud, makes it an ideal testing ground for retina and iris payments (Vidani, Das, Meghrajani, & Chaudasi, 2023). The research suggests these systems can build trust, cut down financial crime, and drive smart city projects forward (Bansal, Pophalkar, & Vidani, 2023). At the same time, plenty of

unanswered questions remain, and future studies have their work cut out for them (Chaudhary, Patel, & Vidani, 2023).

IV. RESEARCH GAP

Research on retina and iris-based biometric payments paints a mixed picture. On one hand, these technologies promise a major leap forward. Banks and payment systems have moved away from PINs and cards, leaning on retina and iris scans for their remarkable accuracy. New breakthroughs—especially in liveness detection and cryptography—have made these methods safer than old-school authentication. Studies from ATMs, UPI platforms, and mobile wallets show that biometric systems slash fraud rates.

But the story isn't all rosy. Biometrics don't solve everything. Spoofing, cyberattacks, and database leaks are still real threats. Researchers keep coming back to the same point: strong safeguards are essential, especially in places like India. The Aadhaar system already stirred up heated debates around privacy and data protection.

There's another angle here. Biometric payments look like a lifeline for underbanked communities, but the tech isn't always accessible to everyone. The literature argues for multi-modal systems—mixing retina, iris, and other options—so nobody gets left out. Adoption rates vary widely, shaped by cultural attitudes, local laws, and infrastructure.

Ahmedabad stands out as a case in point. The city's digital boom, combined with a spike in fraud, makes it an ideal testing ground for retina and iris payments. The research suggests these systems can build trust, cut down financial crime, and drive smart city projects forward. At the same time, plenty of unanswered questions remain, and future studies have their work cut out for them.

V. HYPOTHESIS

This study sets out to see how age shapes the way people think about, use, and trust retina and iris-based biometric payment systems. Here's what we're looking into:

1. Age plays a key role in how often people use digital payments—think UPI, mobile wallets, or internet banking.
2. People's awareness of biometric tech like fingerprint, iris, and retina scanning shifts with age.
3. Age changes how secure people feel about using retina and iris-based payments, especially when compared to the old standbys—PINs or OTPs.
4. Age ties into whether people feel protected from fraud and unauthorized access when they use retina or iris authentication.
5. Age affects whether people would rather use retina or iris authentication instead carrying cards for ATM transactions.
6. Trust in banks and payment providers to keep biometric data safe goes up or down depending on age.

7. Concerns about privacy and the possible misuse of biometric information vary with age.
8. Age connects to the belief that biometric authentication speeds things up and saves time during transactions.
9. Willingness to try out retina or iris-based authentication, if banks offer it, depends on age.
10. People's views on whether customers should pay for biometric technology depend on how old they are.
11. Age shapes whether people think retina and iris-based payment systems work well for all age groups.

Table 1: Validation of Questionnaire

Statements
1. How often do you use digital payment methods such as UPI, wallets, or net banking?
2. Are you aware of biometric authentication methods like fingerprint, iris, and retina scanning in digital payments?
3. Do you believe retina and iris-based payments are more secure than traditional PINs or OTPs?
4. Would you feel safer against fraud and unauthorized access if payments required retina/iris authentication?
5. Would you prefer retina/iris authentication over carrying debit/credit cards for ATM transactions?
6. Do you trust banks and payment providers to securely handle your biometric data?
7. Do you have concerns about the privacy and possible misuse of your biometric information?
8. Do you think biometric authentication would save time and make transactions faster?
9. Would you be willing to adopt retina/iris-based authentication if your bank introduced it?
10. Do you think the cost of implementing biometric technologies should be transferred to customers?
11. Do you think retina/iris-based payments would be convenient for people of all age groups?

12. Are you worried about technical errors or device failures when using biometric authentication?
13. Do you believe retina/iris-based payments can help reduce financial fraud in Ahmedabad?
14. Would you recommend retina/iris-based authentication to your family and friends?
15. Overall, do you see retina and iris-based authentication as the future of secure digital payments in India?

Table 2: Research Methodology

Research Design	Descriptive
Sample Method	Non-Probability - Convenient Sampling method
Data Collection Method	Primary method
Data Collection Method	Structured Questionnaire
Type of Questions	Close ended
Data Collection mode	Online through Google Form
Data Analysis methods	Tables
Data Analysis Tools	SPSS and Excel
Sampling Size	175
Survey Area	Ahmedabad, India
Sampling Unit	Students, Private and government Job employees, Businessmen, Home maker, Professionals like CA, Doctor etc.

VI. DEMOGRAPHIC SUMMARY

Out of the 175 people who took part in the study, most were men—about 81%. Women made up just under 20%. More than half the participants were young adults between 18 and 25, while a quarter were in the 36 to 45 age group. People aged 26 to 35 came next at 14%, and only about 9% were over 45.

When it came to education, nearly 44% were undergraduates. Another 27% had finished higher secondary school, 21% were postgraduates, and 8% held doctoral degrees.

Looking at what they did for a living, students made up the biggest chunk—just over half. Business owners came in at 27%, jobholders at 13%, professionals at 9%, and only a handful—less than 1%—were homemakers.

Family income varied. More than a third reported earning less than ₹50,000 a month. About 32% were in the ₹50,000 to ₹75,000 range, nearly 10% earned between ₹75,000 and ₹1, 00,000, and 22% made over ₹1, 00,000 monthly.

So, this group skews young, educated, and male, with a lot of students and many from middle-income families. These details shape how they approach digital payments and biometric technology, and the data brings out some clear trends in adoption.

CRONBACH ALPHA

Cronbach Alpha Value	No. of Items
0.791	15

The scale's Cronbach's Alpha came in at 0.791 for all 15 items, which tells us the questionnaire holds up well—solid internal consistency. The items actually work together to capture what we're trying to measure. Since the value clears the usual 0.7 cutoff, we can trust the scale and move on with the analysis.

Table 3: Results of Hypothesis Testing

Sr. No	**Alternate Hypothesis**	**Result p =**	**>/ < 0.05**	**Accept/ Reject Null hypothesis**	**R value**	**Relationship**
H01	There is a significant association between age and the frequency of using digital payment methods (UPI, wallets, net banking).	0.000	<	H01 Rejected (Null Hypothesis rejected)	0.899	Strong
H02	There is a significant association between age and awareness of biometric authentication methods like fingerprint, iris, and retina scanning.	0.000	<	H02 Rejected (Null Hypothesis Rejected)	0.000	Weak
H03	There is a significant association between age and belief that retina/iris-based payments are more secure than traditional PINs or OTPs.	0.000	<	H03 Rejected (Null Hypothesis Rejected)	0.000	Weak
H04	There is a significant association between age and feeling safer against fraud and unauthorized access if payments required retina/iris authentication.	0.000	<	H04 Rejected (Null Hypothesis Rejected)	0.000	Weak
H05	There is a significant association between age and preference for retina/iris authentication over carrying debit/credit cards for ATM transactions.	0.000	<	H05 Rejected (Null Hypothesis Rejected)	0.000	Weak
H06	There is a significant association between age and trust in banks/payment providers to securely handle biometric data.	0.000	<	H06 Rejected (Null Hypothesis Rejected)	0.000	Weak
H07	There is a significant association between age and trust in banks/payment providers to securely handle biometric data.	0.000	<	H07 Rejected (Null Hypothesis Rejected)	0.016	Weak

H08	There is a significant association between age and perception that biometric authentication saves time and makes transactions faster.	0.000	<	H08 Rejected (Null Hypothesis Rejected)	0.000	Weak
H09	There is a significant association between age and willingness to adopt retina/iris-based authentication if introduced by the bank.	0.000	<	H09 Rejected (Null Hypothesis Rejected)	0.031	Weak
H10	There is a significant association between age and opinion on whether the cost of implementing biometric technologies should be transferred to customers.	0.000	<	H10 Rejected (Null Hypothesis Rejected)	0.000	Weak
H11	There is a significant association between age and opinion on whether the cost of implementing biometric technologies should be transferred to customers.	0.000	<	H11 Rejected (Null Hypothesis Rejected)	0.008	Weak
H12	There is a significant association between age and worry about technical errors or device failures when using biometric authentication.	0.000	<	H12 Rejected (Null Hypothesis Rejected)	0.002	Weak
H13	There is a significant association between age and belief that retina/iris-based payments can help reduce financial fraud in Ahmedabad.	0.000	<	H13 Rejected (Null Hypothesis Rejected)	0.043	Weak
H14	There is a significant association between age and recommendation of retina/iris-based authentication to family and friends.	0.000	<	H14 Rejected (Null Hypothesis Rejected)	0.000	Weak
H15	There is a significant association between age and perception of retina/iris-based authentication as the future of secure digital payments in India.	0.000	<	H15 Rejected (Null Hypothesis Rejected)	0.985	Strong

VII. DISCUSSION

In this study, I looked at how retina and iris-based payment tech, rolled out by digital payment apps, affects financial scams in Ahmedabad. I paid close attention to how age shapes people's perceptions, whether they use the technology, and how much they trust it. The chi-square results are clear: age matters. It shapes everything from how people behave with digital payments to how aware they are, and whether they're open to using biometrics for authentication.

The data shows a clear link between age and how often people use digital payments like UPI, wallets, and net banking ($p = 0.000$). Younger people dive into these platforms much more often, while older folks tend to stick to traditional methods. This isn't surprising—around the world, younger generations jump on new tech faster. The same goes for awareness of biometric authentication methods—fingerprint, iris, retina scans ($p = 0.000$).

Younger respondents know the most here, too. That gap makes one thing obvious: if we want older users to catch up, targeted awareness campaigns are necessary.

Age doesn't just shape how often people use digital payment tools or how much they know about biometrics. It also colors how safe they feel using things like retina or iris authentication instead of familiar PINs or OTPs ($p = 0.000$)—and whether they trust these methods to guard against fraud ($p = 0.000$). Younger users show more confidence and feel safer with these technologies. They've spent more time with digital tools, and they trust tech safeguards. When it comes to choosing between retina/iris authentication or carrying cards for ATM transactions ($p = 0.000$), the younger crowd prefers the new and convenient. Older users, on the other hand, take a more cautious approach.

Trust in banks and payment providers to safeguard biometric data is another area where age plays a big role ($p = 0.000$). Younger users generally trust these institutions, while older users worry more—probably because they're less familiar with how tech protection works. Age also shapes concerns about privacy and the misuse of biometric data ($p = 0.016$). This isn't just a mild difference—it's a signal that banks and providers need to communicate clearly and build trust, especially with older customers.

The influence of age doesn't stop there. It affects how efficient and time-saving people find biometric authentication ($p = 0.000$). It shapes how willing people are to try retina/iris authentication if their bank introduces it ($p = 0.031$), and how they feel about covering implementation costs ($p = 0.000$). Worries about technical glitches or device failures ($p = 0.002$) lean heavier on older users. Age even sways beliefs about whether retina/iris-based payments can cut down on financial fraud in Ahmedabad ($p = 0.043$), and whether people would recommend these tools to others ($p = 0.000$). Yet, when it comes to seeing retina/iris authentication as the future of secure digital payments in India, age doesn't seem to matter ($p = 0.985$). Here, people across the board share a similar outlook.

In short, age shapes just about every angle of adoption and perception around retina and iris-based payment tech. Younger users lead the way—they use these tools more, understand them better, trust them more, and see more benefits. Older users hesitate. They worry about privacy, technical issues, and costs. To move forward, banks and providers need to craft age-specific strategies: awareness campaigns for older users, easy interfaces for everyone, and security measures that reassure the skeptical. If they get this right, biometric payment tech can play a real part in fighting financial fraud in Ahmedabad.

VIII. THEORETICAL IMPLICATIONS

This study digs into how people actually use digital payment tech and what they think about its security. Age stands out right away—young people aren't just more familiar with digital payments, they also know more about biometric methods. They see retina and iris scanning as fast and useful. The Technology Acceptance Model (TAM) fits here: it's personal perception that decides if someone picks up a new technology or not.

The data also backs up the Diffusion of Innovations (DOI) theory. Younger folks jump on new biometric solutions fast—they're the early adopters. Older people? They're more cautious, sometimes slow to switch, acting as the late majority or laggards. That's a reminder: you can't use a one-size-fits-all approach. If you want everyone on board, you need tailored communication and support.

Trust and risk come up a lot, especially with money involved. Age makes a real difference in how much people trust banks and payment providers to handle their biometric data safely.

Older users worry more about privacy and misuse. It's clear: trust and perceived risk drive adoption, and age shapes both.

The study also sheds light on proactive security behaviors. Age affects the way people view convenience, fraud prevention, and whether they'd recommend retina or iris authentication to others. Demographics don't just color first impressions—they shape real decisions.

In the end, age isn't just a background detail. It drives how people embrace digital payments and biometric security, how much they trust the tech, what risks they notice, and how willing they are to recommend these tools. If you want to design and roll out secure payment systems, you need strategies that take age into account. This research gives a solid foundation for that next step.

IX. PRACTICAL IMPLICATIONS

This study gives clear direction to policymakers, banks, and digital payment providers rolling out retina and iris-based payment tech in Ahmedabad. Age plays a big role in who adopts these systems, who trusts them, and who even knows about them. So, strategies can't be one-size-fits-all. For older users, targeted awareness campaigns and hands-on education make a difference. They worry about privacy, technical failures, and their data getting misused. Tackle those worries head-on, but don't forget to show how much easier and safer biometrics make things.

Younger people? They already use digital platforms, and they're more open to new tech. Banks and payment apps can tap into this by nudging younger customers to spread the word—share positive experiences with family, refer friends, maybe get a reward for it. That kind of social push helps older users feel less anxious about trying something unfamiliar.

But none of this sticks if trust isn't there. Data security sits at the heart of adoption, and people of different ages see risk differently. Banks and service providers need to step up with strong cybersecurity, clear privacy policies, and visible compliance with regulations. Don't keep those efforts in the background—bring them to the front and talk about them. That transparency builds confidence across the board.

Biometric payments should also save time and make life easier. If users can move smoothly between ATMs, POS terminals, and mobile apps, they'll see real benefits and keep using the system.

Cost matters too, especially for older users who might see these new systems as expensive. Banks might have to cover some upfront costs or offer subsidies to make the switch less daunting.

In short, a user-focused, age-aware approach works best. By building trust, raising awareness, showing real convenience, and addressing cost, banks and payment providers can get more people on board, improve digital security, and cut down on fraud in Ahmedabad.

X. CONCLUSION

This study digs into how retina and iris-based payment technologies—rolled out through digital payment apps—are changing the way people in Ahmedabad deal with financial scams.

Age stands out as a big factor. Younger people jump on these new tech options quickly. They trust their banks, feel good about how secure the systems are, and see biometric payments as fast and efficient. Older users? Not so much. They're cautious, worried about privacy, technical glitches, and what might happen if their data falls into the wrong hands.

People across all ages see one clear upside: these biometric payments cut down on fraud, speed up transactions, and make digital payments smoother. Even though older and younger users approach the technology differently, most agree these innovations could reshape digital finance in the years ahead.

On the academic side, the research lines up with established models like the Technology Acceptance Model (TAM), Diffusion of Innovations (DOI), and Trust-Risk frameworks. Age shapes how people accept new tech, what they think about risk, and how much they trust the system. From a practical standpoint, the study pushes for targeted solutions—campaigns tailored by age group, clear messaging on data security, easy-to-use interfaces, and smart management of costs.

Bottom line: retina and iris-based payment tech really can make digital transactions safer and more efficient in Ahmedabad. If banks and payment providers focus on bridging the gap between how different age groups see and use these tools, they'll help build a stronger, more secure digital payments landscape for India.

RECOMMENDATIONS FOR FUTURE RESEARCH/ FUTURE SCOPE OF THE STUDY

This study highlights how retina and iris-based payment technologies can help cut down on financial scams in Ahmedabad, but there's still a lot left to dig into.

1. Widen the Study's Reach- Try bringing in participants from other cities and states—urban, rural, and everything in between. If adoption patterns or trust levels shift from one region to another, we'll see if these findings hold up beyond Ahmedabad.
2. Dig Deeper into the Data- Start by looking at income, education, digital skills, job type, and risk tolerance. These elements shape how people react to biometric payment tech. Understanding them sharpens our sense of who's adopting it, and why.
3. Track Users as They Go- Don't just take a snapshot—watch what happens as people keep using these systems. Does trust build up? Do worries about security drop off? Older users matter here too—see if their skepticism fades as they get more comfortable.
4. Measure Awareness and Training Efforts- See if well-designed awareness campaigns and training sessions actually boost adoption and trust, especially among older users worried about privacy, data security, or technical hiccups.
5. Put the Tech to the Test- Study how reliable and secure retina and iris authentication really are. Dig into device failures, possible spoofing attacks, and system errors. You'll get a better sense of both user confidence and the tech's actual strength.
6. Stack up Different Biometric Methods- Run studies that pit fingerprint, facial recognition, voice, and retina/iris authentication against each other. Find out which ones people prefer, what feels safest and easiest, and which barriers slow down adoption. This helps providers pick the right tools for the job.
7. Unpack Psychological and Behavioral Forces- Take a close look at what really drives people: perceived risk, trust in their bank, convenience, security concerns. Frameworks

like the Technology Acceptance Model and Trust-Risk models help break this down so we're not just guessing what's in users' heads.

8. Measure Real-World Fraud Impact- Lastly, does retina or iris-based payment actually reduce fraud? Find out. Banks, policymakers, and payment platforms need solid evidence to make digital payments safer for everyone.

REFERENCES

[1] Bhatt, V., Patel, S., & Vidani, J. N. (2017, February). START-UP INDIA: A ROUGH DIAMOND TO BE POLISHED. National Conference on Startup India: Boosting Entrepreneurship (pp. 61-67). Pune: D.Y. Patil University Press.

[2] Biharani, S., & Vidani, J. N. (2018). ENTREPRENEURSHIP: CAREER OPPORTUNITY HAS NO GENDER DISCRIMINATION. Compendium of Research Papers of National Conference 2018 on Leadership, Governance and Strategic Management: Key to Success (pp. 101-104). Pune: D. Y Patil University Press.

[3] Dhere, S., Vidani, J. N., & Solanki, H. V. (2016, November). A SURVEY ON THE TOWARDS SATISFATION LEVEL OF THE CUSTOMER SHOPPING MALL'S: AN ANALYTICAL STUDY. International Multidisciplinary Journal Think Different, 3(24), 45-50.

[4] Mala, Vidani, J. N., & Solanki, H. V. (2016, November). GREEN MARKETING-A NEw WAY OF MARKETING: A REVIEW APPROACH. International Multidisciplinary Journal Think Different, 3(24), 40-44.

[5] 4. 4. Modi, R., Harkani, N., Radadiya, G., & Vidani, J. N. (2016, August). Startup India: Even Diamonds start as Coal. NTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, 2(8), 111-116.

[6] Niyati, B., & Vidani, J. N. (2016, July). Next Generation Children: Smarter or Faster. NTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, 2(7), 110-114.

[7] Odedra, K., Rabadiya, B., & Vidani, J. (2018). AN ANALYSIS OF IDENTIFYING THE BUSINESS OPPORTUNITY IN AGRO and CHEMICAL SECTOR - WITH SPECIAL REFERENCE TO AFRICAN COUNTRY UGANDA. Compendium of Research Papers of National Conference 2018 on Leadership, Governance and Strategic Management: Key to Success (pp. 96-100). Pune: D.Y Patil University Press.

[8] Pathak, K. N., & Vidani, J. N. (2016). A SURVEY ON THE AWARENESS SATISFACTION AS WELL ASTO KNOW THE LEVELoF OF THE ONLINE SHOPPING AMONG THE PEOPLE OF AHMADABAD CITY. Governance in E-commerce: Contemporary Issues & Challenges (pp. 261-275). Ahmedabad: GTU.

[9] Pradhan, U., Tshogay, C., & Vidani, J. N. (2016, July). Short Messages: It's Effect on Teenager's Literacy and Communication. NTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, 2(7), 115-120.

[10] Rathod, H. S., Meghrajani, D. I., & Vidani, J. (2022, December). Influencer Marketing: A New Marketing Communication Trend. Shodhsamhita, VIII (12(II)), 155-167.

[11] Sachaniya, C., Vora, H., & Vidani, J. (2019). A Study on Identifying the Gap between Expected service and Actual Service with Special Reference to Suk Sagar Gir Resort, Sasan. In P. Rijwani, S. Shome, & D. Danak (Ed.), BUSINESS, ECONOMY AND ENVIRONMENT: CORPORATE PERSPECTIVES (pp. 162-169). Ahmedabad: Himalaya Publishing House Pvt. Ltd.

[12] Saxena, M., & Vidani, J. N. (2023). MBA Chai Wala. In M. R. Dixit, S. Bist, & S. Shah, Searching Alternativies (pp. 22-32). Ahmedabad: Routledge - imprint of Taylor & Francis group.
[13] Singh, P. K., & Vidani, J. N. (2016, November). PROBLEMS AND PROSPECTS OF AGRICULTURE MARKETING IN INDIA. International Multidisciplinary Journal Think Different, 3(22), 9-16.
[14] Singh, P. K., Vidani, J. N., & Nagoria, V. S. (2016, July-September). Waste Management: Inspire Today for A Better Tomorrow. Journal of Basic and Applied Engineering Research, 3(10), 921-926.
[15] Solanki, H. V., & Vidani, J. N. (2016, November). A NEW ERA OF E-VYAPAR IN 21ST CENTURY: A REVIEW APPROACH. INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH, 5(11(2)), 61-77.
[16] Solanki, N., & Vidani, J. N. (2016, January). THE STUDY LEGAL ASPECTS OF TRADE IN ETHIOPIA. ZENITH International Journal of Multidisciplinary Research, 6(1), 226-284.
[17] Sukhanandi, S., Tank, D., & Vidani, J. N. (2018). ANALYSIS OF THE IMPACT OF WORK LIFE BALANCE ON WORKING WOMEN LEADER IN INDIA. National Conference 2018 on Leadership, Governance and Strategic Management: Key toSuccess (pp. 77-80). Pune: D.Y.Patil University Press.
[18] Vasveliya, M., & Vidani, J. (2019). A Study on Analyzing Gap between Expected and Actual Customer Satisfaction Regarding Royal Enfield's Features and Services. In P. Rijwani, S. Shome, & D. Danak (Ed.), BUSINESS, ECONOMY AND ENVIRONMENT: CORPORATE PERSPECTIVES (pp. 79-85). Ahmedabad: Himalaya Publishing House Pvt. Ltd.
[19] Vidani, J. N. (2015, December). "THE STUDY OF THE CONCEPTS OF PERSONALITY TRAITS, VALUES, SKILLS AND PERCEPTION OF DR.MANMOHANSINGH. The Indian Writer's e – Journal, 1(1), 1-14.
[20] Vidani, J. N. (2015, Novemmber). Self-Aid Group – A Preeminent way for Bucolic Female Empowerment. International Journal of Advance Engineering and Research Development, 2(11), 351-360.
[21] Vidani, J. N. (2015, December). THE STUDY OF INVESTMENT PATTERN OF THE PEOPLE OF BHAVNAGAR DISTRICT. The Indian Writer's e – Journal, 1(1), 1-26.
[22] Vidani, J. N. (2015, December). THE STUDY OF PESTLE ANALYSIS IN KERALA STATE. ZENITH International Journal of Multidisciplinary Research, 5(12), 33-50.
[23] Vidani, J. N. (2016, November). Fake Opportunities and Real Challenges of an Indian Women Entrepreneurs: A Review Approach. International Journal of Multidisciplinary Educational Research, 5(11(3)), 224-237.
[24] Vidani, J. N. (2016). IS ENTREPRENEURSHIP A GENDER BLIND (PART II). Indian Journal of Technical Education (IJTE) - Special Issue for ICWSTCSC-2016, 25-33.
[25] Vidani, J. N. (2016, December). Roles of a Bhartiya Nari Vyapari: A Case study review Approach. International Journal of Management, IT & Engineering, 6(12), 328-341.
[26] Vidani, J. N. (2016, September). Rural Women Entrepreneurship: "Nari Bani Vyapari". International Journal of Management and Research, 1, 208-213.
[27] Vidani, J. N. (2018). Export and Import Procedures (Vol. 1). Online: Educreation Publishing.
[28] Vidani, J. N. (2018). MERGER AND AQUIsITIONS: A CASE FROM INDIAN TELECOM SECTOR VODAFONE & IDEA. Compendium of Research Papers of National Conference 2018 on Leadership, Governance and Strategic Management: Key to Success (pp. 105-108). Pune: D.Y Patil University Press.
[29] Vidani, J. N. (2018). Overview of Opportunities and Challenges in Marketing Strategies of Ecopreneurs for their Eco-Prenrurial Products in the Markets of

Saurahtra Region. In B. UNNY, D. N. BHATT, & D. S. BHATT (Ed.), Transformation Through Strategic and Technological Interventions (pp. 159-167). Ahmedabad: McGraw Hill Education (India) Private Limited.

[30] Vidani, J. N. (2019). INFLUENCER MARKETING: A NEW TREND. Nafional Conferenee on "Multidisciplinary Research in Socelal Seienes & Management Studies. 6, pp. 344-353. Pune: D.Y Patil Institute of Management Studies.

[31] Vidani, J. N. (2020). ROLE OF WOMEN IN AGRICULTURE SECTOR OF INDIA. In P. (. Mateen, WOMEN EMPOWERMENT & ECONOMIC DEVELOPMENT (pp. 32-47). Kanpur: International Publications.

[32] Vidani, J. N. (2022). Digital Marketing for Business in #hashtag era (Vol. 1). Delhi, India: Publishing Expert.

[33] Vidani, J. N., & Das, D. S. (2021, August). A Review on Evolution of Social Media Influencer Marketing: Reflection on Consumer Behaviour and Consumer's Decision-Making Process. Turkish Online Journal of Qualitative Inquiry (TOJQI). Retrieved from https://www.tojqi.net/index.php/journal/issue/view/51

[34] Vidani, J. N., & Dholakia, A. (2020). An Introspective Study on Retail Sector The Current Scenario in Gujarat and India. In R. B. Chauhan, Management and Innovation: Research Study (pp. 1-15). Kanyakumari: Cape Comorin Publisher.

[35] Vidani, J. N., & Pathak, K. N. (2016). A SURVEY ON AWARENESS AND SATISFACTION LEVEL OF THE CONSUMERS OF ONLINE GIFTING WITH SPECIAL REFERENCE T0 AHMADABAD CITY. Governance in E-commerce: Contemporary Issues &Challenges (pp. 121-135). Ahmedabad: GTU.

[36] Vidani, J. N., & Plaha, N. G. (2016, November). SWACHH BHARAT: CSR INITIATIVE BY INDIAN CORPORATES. International Multidisciplinary Journal Think Different, 3(22), 44-50.

[37] Vidani, J. N., & Plaha, N. G. (2017). AGRIPRENEURSHIP: A REINCARNATION OF INDIAN AGRICULTURAL SECTOR. Proceedings of the International Conference on Enhancing Economic Productivity and Competitiveness through Financial and Monetary Reforms (pp. 154-159). Ahmedabad: GTU.

[38] Vidani, J. N., & Singh, P. K. (2017). To study the effect of marketing on awareness and the use of contraceptive pills in the rural areas with special Reference to Ahmedabad District. Services in Emerging Markets (pp. 254-265). Ahmedabad: Emerald.

[39] Vidani, J. N., & Solanki, N. (2015, December). THE STUDY OF FUNDAMENTAL CONCEPTS OF MANAGEMENT FOCUSING ON POSDCORB ANALYSIS - PARLE INDIA PVT. LTD. EXCEL International Journal of Multidisciplinary Management Studies, 5(12), 45-56.

[40] Vidani, J. N., Chack, P. K., & Rathod, D. N. (2017, February). STARTUP INDIA: A CHALLENGING WAY OF THRONES. National Conference on startup India: Boosting Entrepreneurship (pp. 111-118). Pune: D. Y. Patil University Press.

[41] Vidani, J. N., Meghrajani, I., & Siddarth, D. (2023, May). Unleashing the Power of Influencer Marketing: A Study on Millennial Consumer Behaviour and its Key Antecedents. JOURNAL OF EDUCATION: RABINDRA BHARATI UNIVERSITY, XXV(6), 99-117.

[42] Vidani, J., Jacob, S., & Patel, M. (2019, July - September). MENTAL HEALTH START-UP: MOODCAFE. Economic Challenger: An International Journal, 21(84), 35-42.

[43] Bansal, A., Pophalkar, S., & Vidani, C. (2023). A Review of Ed-Tech Sector in India. International Journal of Management Analytics (IJMA), 1(1), 63-84.

[44] Chaudhary, N., Patel, V., & Vidani, C. J. (2023). A Review of Non-Technical Training Programmes Conducted by Corporate Trainers for IT Companies. International Journal of Management Analytics (IJMA), 1(1), 85-110.

[45] Patel, V., Chaudhary, N., & Vidani, C. J. (2023). A Study on Awareness of Various Non-Technical Training Programmes Conducted by Corporate Trainers for IT Companies in Ahmedabad. International Journal of Management Analytics (IJMA), 1(1), 111-132.
[46] Sharma, S., & Vidani, C. J. (2023). To Study the Consumer Attitude Towards Purchase Intention of Online Courses on Udemy Using Co-Relation with Reference to English Speaking and Excel Among Gen-Z in Ahmedabad. International Journal of Management Analytics (IJMA), 1(1), 193-212.
[47] Sharma, S., & Vidani, C. J. (2023). To Study the Consumer Attitude Towards Purchase Intention of Online Courses on Udemy Using Regression with Reference to English Speaking and Excel Among Gen-Z in Ahmedabad. International Journal of Management Analytics (IJMA), 1(2), 213-234.
[48] Vidani, J. N., Das, S., Meghrajani, I., & Singh, G. (2023, August). Influencer Marketing and Gendered Consumer Behavior: An Analysis of Clothing Purchases across Different Fashion Categories. Sodhsamhita, 137-157.
[49] Vidani, J., Das, S., Meghrajani, I., & Chaudasi, C. (2023). Unveiling the Influencer Appeal: A Gender-Centric Exploration of Social Media Follower Motivations. Rabindra Bharati Journal of Philosophy, 182-203.
[50] Mahajan, H., & Vidani, J. (2023). Packaging strategies: Outlook on consumer buying behaviour for FMCG products. Journal of Management and Entrepreneurship, 17(4), October - December 2023.
[51] Saxena, M., & Vidani, J. (2023). MBA Chai Wala. In M. R. Dixit, S. Bist, & S. Shah, Searching Alternativies (pp. 22-32). Ahmedabad: Routledge - imprint of Taylor & Francis group.
[52] CARD-LESS ATM TRANSACTION USING RETINAL & FACE RECOGNITION USING DEEP LEARNING ALGORITHM. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets42679.
[53] Puri, G., & Gupta, H. (2016). ID Based Encryption in Modern Cryptography. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. https://doi.org/10.1145/2905055.2905221.
[54] Galhotra, B., Bajaj, S., Jatain, A., & Jaglan, V. (2024). Enhancing Automated Payments: Impact of Iris Technology's in UPI Transactions. 2024 4th International Conference on Soft Computing for Security Applications (ICSCSA), 487-491. https://doi.org/10.1109/ICSCSA64454.2024.00084.
[55] Arepalli, G., Bhavana, P., Krishna, Y., & Surendrababu, C. (2024). Enhancing Transaction Security through Iris Recognition. 2024 International Conference on Expert Clouds and Applications (ICOECA), 684-688. https://doi.org/10.1109/ICOECA62351.2024.00124.
[56] Rashidi, F., Mohsini, M., & Mega, B. (2024). A framework for security improvement on usage of mobile money application based on iris biometric authentication method. Information Security Journal: A Global Perspective, 33, 678 - 690. https://doi.org/10.1080/19393555.2024.2347240.
[57] Krishnakumar, B., KishoreKumar, M., & Karthikeyan, L. (2015). Implementation of IRIS recognition for Securing Online Payment. International journal of scientific research in science, engineering and technology, 1, 298-302.
[58] Liébana-Cabanillas, F., Muñoz-Leiva, F., Molinillo, S., & Higueras-Castillo, E. (2022). Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint. Financial Innovation, 8. https://doi.org/10.1186/s40854-021-00328-z.