Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

51

Adoption of Passwordless Banking: Understanding Consumer Behaviour

Ramya. R[1]

Assistant Professor, Department of Commerce, M.O.P. Vaishnav College for Women (Autonomous), Nungambakkam, Chennai, India

Sriya Vasudevan[2]

II.B. Com, Department of Commerce, M.O.P. Vaishnav College for Women (Autonomous), Nungambakkam, Chennai, India

Dyuti Srinivasan[3]

I.B. Com, Department of Commerce, M.O.P. Vaishnav College for Women (Autonomous), Nungambakkam, Chennai, India

ABSTRACT

Ever since digitalisation took the fore-front in the developmental process of India, it has become increasingly evident that technology is the future that will replace most of the mundane tasks performed by us. The banking sector poses as a prime example of this transformation. With the shift from in-person banking practices to digitalised payments through unified payments interface (UPI), India has grown to become a digital-transaction oriented nation. The rise of digital transactions has posed a serious threat to the current generation- Authentication. Authentication and verification of one's identity to perform digital banking practices still to date rely on password-authorised access. As time flows this has proven to be tedious to remember and more prone to phishing and hacking. A Viksit Bharat envisions a change towards a Passwordless banking approach providing a more secure and hack-free platform for consumers. This paper aims to understand the concept of Passwordless banking and analyse the consumer behaviour with regards to Passwordless banking and security concerns.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

KEYWORDS: - Banking industry, Passwordless, Authentication, Digitalisation

INTRODUCTION

Viksit Bharat 2047 focuses on utilising the nation's resources towards utmost optimisation. The Government of India has introduced schemes such as Pradhan Mantri Jan Dhan Yojana which investigates the creation of a bank account for every single Indian in the country. The scheme has helped banking services to reach every corner of India- right from lower income groups to high income groups of the country. This has propelled the fintech-ecosystem to thrive in India.

Many of the banking services can be carried out just via a mobile phone providing for a seamless banking experience to the citizens. This being the scenario in the banking sector, there is a growing need for simplification of credential verification with security. People find it difficult to set strong passwords as per password policy while this gets complicated for people with more than one bank account. In addition to this, it also creates an ironic situation that people protect all their passwords with a password.

Password authentication and one-time password (OTP) verification pose a serious threat of hacking. With the rising cyber-crime rates, it is necessary that a strong security system is put in place. The vulnerability of this traditional system has prompted the introduction of recent technological developments as alternatives to password verifications making authentication and security seamless. To achieve complete security in digital banking transactions, it is very much essential that India taps the concept of Passwordless-banking and makes it a reality by 2047.

OBJECTIVES

1. To understand the concept of Passwordless Banking.
2. To analyse the consumer behaviour with respect to Passwordless Banking.
3. To highlight the benefits of transcending towards passwordless banking for a Viksit Bharat

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

HYPOTHESIS

1. H_0: Demographic consumer attributes do not influence the preference of password-based authentication.

   H_1: Demographic consumer attributes influence the preference of password-based authentication.

2. H_0: The perception towards accounts being hacked, biometrics usage, difficulty in storing and setting passwords have no significant impact on the preference between passwordless and password banking.

   H_1: The perception towards accounts being hacked, biometrics usage, difficulty in storing and setting passwords have a significant impact on the preference between passwordless and password banking.

REVIEW OF LITERATURE

According to the India Brand Equity Foundation (IBEF) report of July 2024, India has one of the largest growing fintech bases. With the RBI leading the forefront in the banking industry, this sector has become regularised and has increased its capital earnings to a significant rate. Being one of the 3rd largest fintech based countries with an estimate to grow towards 150 million USD by 2025, India's banking industry has embraced the advent of changes in technology and has clearly adapted to it and has been providing for consumers with customised services. With the emergence of various schemes such as the Pradhaan Mantri Jan Dhan Yojana and Post-payments banks being tied up with the digital payment technology has immensely added in the better accessibility of financial services to the citizens of India. Currently with a figure of around two thousand recognised fintech businesses in India, the digital payments system has evolved to be a breakthrough in the finance industry with the Immediate Payment Service and the Unified Payments Interface leading the forefront of this quantum leap towards harnessing the power of technology.

According to HP Singh article (published in Times of India on March 18, 2023), the banking sector has undergone a remarkable transformation, driven by the rise of digitization. Once defined by long waits at bank branches and other tedious processes, bank customers can now do everything online, up to and including paying bills and transferring funds to an account. Digitization also started to really take root during the pandemic as everyone sought to turn to digital banking options. Primary benefit of digitization is the ability for banks to collect and analyse an increasing volume of customer data, gaining intelligence and insight on customer habits. Leveraging the data with analytics and artificial intelligence- AI, enables banks to develop products and services that are personalised. Additionally, it helps in detecting patterns and anomalies in customer transactions, flagging suspicious activities for further investigation, thus enhancing security. IoT technology, through devices like ATMs, mobile banking apps, point of sale terminals optimises operations and enhances cybersecurity. Overall, digitization in banking is revolutionising financial services, promoting financial inclusion, and driving economic growth by making banking more accessible and efficient.

According to an article by Pedro Martinez (published in Thales Group, on 11th October 2022), Multi-Factor Authentication (MFA) plays a critical role in securing user access to financial services. Service providers ensure identity by verifying three factors: *Knowledge Factor* (passwords, PINs), *Possession Factor* (cards, tokens, phones), and *Inherence Factor* (biometrics). While no single factor is enough for security, combining at least two creates Strong Customer Authentication (SCA). In the late 80s and early 90s, remote financial services like e-banking required only a username and password, this specific authentication method was a less secure option than being authenticated at an ATM, where card and PIN provided two-factor authentication. By the mid-90s, financial institutions introduced OTP tokens, reinforcing security but impacting user experience. As smartphones became more common, banks started using SMS-based OTPs (One-Time Passwords) for authentication. This led to digital banking evolving rapidly, and since then banks have been working to balance security with a smoother and more convenient user experience.

According to Deloitte report "Next Frontier in Security: Passwordless Authentication" (published in June 2023), passwords are increasingly recognized as a critical security risk, contributing to most data breaches and application attacks. The report highlights that 67% of application attacks and a whopping 82% of data breaches involve stolen credentials, primarily due to user password fatigue and reuse. This has led many organisations to adopt Multi-Factor Authentication (MFA) to increase security, yet MFA often introduces additional user friction and is susceptible to attacks such as prompt bombing and phishing. A more solid substitute for this may be the passwordless authentication from Fast Identity Online (FIDO) Alliance which eliminates passwords entirely. This uses device-based biometrics or hardware token authentication for a more secure and user-friendly experience. It also outlines several benefits of transitioning to passwordless systems, including improved security, reduced user frustration, and lower operational costs related to password resets. Moving to passwordless authentication is not just a technology change, but also a mindset shift for all stakeholders.

According to the article by Riya Sandhu (published in Indian Journal of Science and Technology in November 2019) the evolution of authentication systems in information security is examined, throwing light on the vulnerabilities of traditional password-based mechanisms. It highlights how passwords, despite being one of the oldest methods of authentication, remain a significant target for attackers due to the ease of obtaining them. Attackers have developed sophisticated methods such as brute force attacks, password replay, and man-in-the-middle attacks to exploit password-based systems, often compromising sensitive information. Powerful computation can attempt billions of password combinations in seconds. Password replay attacks take advantage of communication to gain access to accounts, while man-in-the-middle attacks allow hackers to put themselves in between two users to collect private data. Companies like Microsoft have recognized that passwords have limitations and have begun to shift toward a passwordless situation for better security. One of the solutions to this security problem is through *multi-factor authentication* which has users verify through multiple steps such as swiping a card, creating a one-time password, or biometric recognition. Microsoft's Windows Hello is a prime example of this and uses biometric data such as fingerprints, facial recognition, or iris reading to confirm the user and backend without

passwords. It also highlights the importance of users knowing the benefits of passwordless technologies. User awareness will provide the avenue for organisations to lead to greater adoption of faster, safer, and more effective user security. Systems integrate features like magic links, codes, and biometric recognized identification and account verification authentication. Passwordless technologies represent a vital evolution in cybersecurity technologies.

According to Anushka Sengupta (published in May 2023 in The Economics Times report "Will Passkeys Make BFSI Passwordless?") Passwords have long been the cornerstone of digital security. Passwords are easy to forget, steal, or hack, which means that personal information still may not be safe. To make matters worse, individuals regularly jot down passwords on paper or use weak or easily guessed passwords, such as their children's names or favourite sports teams, which only compounds the situation. Enter *Passkeys*, a simple, and more secure option for digital banking authentication. Passkeys are based on the FIDO2 standard and utilise cryptography and biometrics to provide enhanced protection against phishing and data breaches. Passkeys are the most innovative alternative to passwords and will help ensure that a user's digital identity is more effective than passwords alone. Amit Goel emphasised that passkeys solve security challenges associated with passwords, while presenting a cheaper alternative. Storing credentials on devices rather than storing them on a server address both the risk of hacks and reliance on costly one-time passwords (OTPs). For the BFSI sector, this means enhanced security and reduced operational costs, paving the way for a more secure and economically efficient digital banking experience.

According to Viral Parmar, Harshal Sanghvi, Riki Patel, Abhijit Pandya (published in April 2022 in Research Gate) as the world transitions towards a digitalised economy, passwords have proven to be a significant threat in the banking industry. With technology developing it has become easy to phish and hack passwords hence making us ponder the credibility of safety they carry. It is hence necessary that the transactions are secured with end-to-end encryption technology. This can ultimately help provide enhanced customer experience, and improved security to potential clients. Upon comparison of the various traditional and modern technology upgrades in banking authentication it can be clearly observed that the password-less banking concept has very much taken the fore-front and has helped in improving

customer satisfaction in great length. The article has touched upon various passwordless banking and traditional banking practices such as social login authentication and one-time passwords and has clearly evaluated each one of them based on their advantages and disadvantages. The article also discusses in detail biometric, facial recognition and retinal authentication technology. The study concluded that passwordless technology is the new future and will soon replace the traditional password banking operations.

According to Tapesh Bhatnagar (published in March 2024 in Financial Express) India's digital landscape is evolving rapidly, with smartphone usage soaring from 15% to 66% in eight years. As a result, digital transactions soared to approximately $1.63 billion from $0.25 billion between FY 2017-18 and FY 2022-23. However, traditional means of digital authentication through passwords and SMS-based OTPs are now becoming increasingly vulnerable when it comes to cybercrime. In response to this, the RBI Governor introduced a framework to explore more secure, alternative means of authentication. Transitioning from passwords to biometrics and passwordless authentication standards, such as FIDO, will eventually result in enhanced security and more effortless user experiences through biometric authentication instead of passwords. With its long history of expertise in security technology, Giesecke + Devrient (G+D) takes the lead in driving this transition by proposing solutions that combine biometric and NFC technologies into secure and seamless digital user experiences. A transition to passwordless authentication is a pivotal step in digital security, to ensure that the future is safer and simpler.

According to BIO-Key International Inc (published in April 2024 on LinkedIn) Biometric verification is swiftly emerging as a key driving factor of modern digital security, owing to the increasing need for strong security across an array of industries. It is observed that disciplines, including, but certainly not limited to, banking, healthcare, and government have begun to integrate biometric technology, including fingerprints, facial recognition, irises, and voice verification, to enhance security and protect sensitive data. Their solutions not only boost existing security parameters, but also provide convenience by eliminating the need for passwords or PINs. BIO-Key discusses that the implementation of biometrics with AI and ML is fundamentally changing authentication systems in ways that are adaptive and intelligent. AI

friendly biometric solutions, which can identify unusual behaviours, result in additional layers of security. Despite the advantages to biometric systems, BIO-Key outlines challenges that this aspect of digital security incurs, primarily with respect to privacy and data security. Issues of data breaches and biometric misuse present serious hurdles for biometric applications, necessitating discussions concerning ethical practices and thorough legislation patterns. The company also points out the need for standardised frameworks to ensure that biometric data is stored and processed securely. As the adoption of biometrics continues to rise, BIO- Key stresses the importance of balancing innovation with ethical considerations to ensure user trust and system integrity.

According to Narasimha Raju (published in March 2023 in CXOToday) 1Kosmos is a worldwide leader in identity proofing and passwordless authentication and is progressing significantly in India's digital market. Soon after, major Indian companies, such as Union Digital, and Vodafone Idea, began deploying the BlockID platform and through its implementation, 1Kosmos has taken measures to stop identity impersonation, account takeovers, and fraud while reaching millions of users. The BlockID platform provides strong and passwordless authentication which ensures safe and seamless access for employees and customers alike. With increasing demand throughout various sectors, 1Kosmos' national footprint has taken hold while providing clients with a simple and efficient approach to identity management. Their technology has laid the groundwork for frictionless identity verification and authentication while addressing the challenges of the password experience. As stated by Siddharth Gandhi, COO of 1Kosmos, the integration of the technology has been led by visionary CIOs and CISOs who appreciate the security concerns created by complex passwords and the need for passwordless solutions. Given recognitions from leading analyst firms like Gartner and KuppingerCole, and appreciation of their market momentum as a verified identity and passwordless authentication leader, 1Kosmos' continued investment in India's multiplying cloud and digital market accelerates initiatives such as Skill India for a secure digital future. 1Kosmos continues to innovate simplified identity management, in a secure fashion, all the way through.

According to Karan Choudhary (published in April 2023 in MojoAuth) Across multiple industries, especially in the SaaS and eCommerce sectors, passwordless authentication is gaining momentum due to increased security and convenience, as well as cost benefits. Passwordless authentication can now be accomplished through biometrics, magic links, or security keys, eliminating the use of vulnerable passwords and the risk of a data breach. The change from a password-based system to a passwordless system fixes several key problems: First, it greatly diminishes the exposure of credential theft and phishing attacks that are prevalent in a password-based system. Secondly, users enjoy the advantage of not having to navigate the complexities of password management, resulting in a more positive user experience. From an organisational standpoint, businesses save money with the decrease of support and maintenance costs associated with password resets, forgotten passwords, and account recovery. Organisations also have the improved responsibility of protecting data due to the significant avoidance of regulatory compliance issues associated with passwords, such as with GDPR or HIPAA. Moreover, advancements such as multi-factor authentication (MFA) standards; and the emergence of standards such as FIDO2 have provided for advancements that are the next-generation of intuitive, secure user authentication to drive both security and user loyalty. The demonstration of upcoming organisations adopting passwordless authentication standards is not only a result of increasing security challenges, but a proactive approach to improving security through a more efficient user-friendly and access-friendly system authentication.

According to HYPR (published in April 2021 in Cybersecurity Insiders) The emergence of passwordless multi-factor authentication (MFA) is becoming more significant due to the focus on mitigating credential-based attacks and improving user experience. According to recent data, 91% of respondents highlight the prevention of such attacks as the primary reason for adopting passwordless MFA, while 64% ranked improved user experience as the most significant reason. Despite a significant interest, 61% of organisations continue to implement MFA solutions based on shared secrets, like passwords or one-time passwords (OTPs), suggesting a disconnect between ideal practice and current practice. Further, there is a demand for a more user-friendly experience (UX), which is reflected in the fact that 48% of organisations do not currently have a passwordless solution; although, 36% of organisations

use smartphone-based MFA technologies. Moreover, 67% of enterprises say they have low UX expertise with smartphones being the most favoured method of MFA. Additionally, when enterprises are transitioning to passwordless systems, 94% of respondents say this standardisation through an accepted framework, such as FIDO, is necessary, both for continuous enterprise-ready solutions and future-proof designs to integrate easily into their existing IT environments. Even though interest continues to increase towards passwordless authentication, only 24% of Gen Z users use password management applications, and interest varies by age group. The report noted a considerable shift to the passwordless MFA technology market, suggesting that as the technology moves to the mainstream, it appears as though very often the shift to a passwordless MFA solution is ahead of expectations, as in both consumer and workforce applications there is a growing awareness of its potential impact and benefits.

According to Assumpta Ezugwa, Elochukwu Ukwandu, Celestine Ugwu, Modesta Ezema, Comfort Olebara, Juliana Ndanagu, Lizzy Ofusori and Uchenna Ome (published in Science Direct on 29 May 2023) Passwordless technology has been in the development and many people are yet to be familiarised with the concept. This technology is said to very soon replace the traditional password-based technology and provide a more seamless-user friendly experience with high end security to the consumers. Upon a survey conducted by them to understand the consumer experience with handling password-based technology. Though a definite consensus of passwordless being superior over passwords was not reached, they were able to navigate and understand the possible factors that could impact people's mindsets towards handling passwords. They found that people above 60 find it difficult to remember passwords and prefer passwordless technology over passwords. However, their study was not conclusive in nature as they did not focus on probable areas that might impact adaptation to passwordless technology such as handling of passwords, password hygiene culture etc. Hence it was concluded that consumer experience is relative in nature and varies from different geographical, cultural, social environments and the various technological tools exposed to the people.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

RESEARCH METHODOLOGY

The research methodology methods used in this survey include primary data and secondary data. Primary sources include a survey through a Google form – a questionnaire that was prepared to understand the consumer behaviour towards authentication of banking services. The questionnaire also focused on providing an awareness about Passwordless banking to the respondents as well. The sample size of the research is 131 respondents. Secondary data was collected from sources such as published articles, research papers and various websites and blogs. The analysis was done based on results received via Chi-square test and Multiple Regression on SPSS software. Further, the results of the survey were studied with the help of bar charts.

DATA ANALYSIS AND INTERPRETATION

Table1: Table showing Association between age and shift towards passwordless banking

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.301[a]	3	.231
Likelihood Ratio	4.670	3	.198
Linear-by-Linear Association	.009	1	.924
N of Valid Cases	131		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .55.

Table 1 indicates the Pearson Chi-Square test statistic to be 4.301. The p-value of Pearson's chi-square test statistic is 0.231, which is more than the 5 percent value of significance. This indicates the null hypothesis of age of a person not influencing the decision of moving towards passwordless banking can be accepted. Thus, it can be concluded that there exists no significant association between them. Hence the alternate hypothesis is ruled out.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Table 2: Table showing Association between Gender and shift towards passwordless banking			
	Value	**df**	**Asymptotic Significance (2-sided)**
Pearson Chi-Square	1.050[a]	1	.306
Continuity Correction	.208	1	.648
Likelihood Ratio	.939	1	.333
Linear-by-Linear Association	1.042	1	.307
N of Valid Cases	131		

Table 2 indicates the Pearson Chi-Square test statistic to be 1.050. The p-value of Pearson's chi-square test statistic is 0.306, which is more than the 5 percent value of significance. This indicates the null hypothesis of gender of a person not influencing the decision of moving towards passwordless banking can be accepted. Thus, it can be concluded that there exists no significant association between them. Hence the alternate hypothesis is ruled out.

Table 3: Table showing Association between Education and shift towards passwordless banking			
	Value	**df**	**Asymptotic Significance (2-sided)**
Pearson Chi-Square	4.000[a]	3	.261
Likelihood Ratio	5.451	3	.142
Linear-by-Linear Association	.069	1	.793
N of Valid Cases	131		
a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .40.			

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Table 3 indicates the Pearson Chi-Square test statistic to be 4.000. The p-value of Pearson's chi-square test statistic is 0.261, which is more than the 5 percent value of significance. This indicates the null hypothesis of education levels of a person not influencing the decision of moving towards passwordless banking can be accepted. Thus, it can be concluded that there exists no significant association between them. Hence the alternate hypothesis is ruled out.

Table 4: Table showing Association between Employment and shift towards passwordless banking

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.881[a]	6	.930
Likelihood Ratio	2.483	6	.870
Linear-by-Linear Association	.141	1	.707
N of Valid Cases	131		

a. 8 cells (57.1%) have expected to count less than 5. The minimum expected count is .03.

Table 4 indicates the Pearson Chi-Square test statistic to be 1.881. The p-value of Pearson's chi-square test statistic is 0.930, which is more than the 5 percent value of significance. This indicates the null hypothesis of employment status of a person not influencing the decision of moving towards passwordless banking can be accepted. Thus, it can be concluded that there exists no significant association between them. Hence the alternate hypothesis is ruled out.

Table 5: Table showing Association between Income and shift towards passwordless banking

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.739[a]	3	.864
Likelihood Ratio	1.271	3	.736
Linear-by-Linear Association	.207	1	.649
N of Valid Cases	131		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .55.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Table 5 indicates the Pearson Chi-Square test statistic to be 0.739. The p-value of Pearson's chi-square test statistic is 0.864, which is more than the 5 percent value of significance. This indicates the null hypothesis of employment status of a person not influencing the decision of moving towards passwordless banking can be accepted. Thus, it can be concluded that there exists no significant association between them. Hence the alternate hypothesis is ruled out.

In recent times, individuals across different demographic categories are technology-friendly. People are now familiar with modern authentication methods. With smartphones being a necessity, people from all demographics are used to fingerprint scanning or face recognition. In addition, regulatory frameworks mandate the use of strong, modern authentication methods for everyone. When such a framework affects all users equally, demographic distinctions become less relevant in the decision to adopt passwordless technologies. Hence, we can conclude that demographic consumer attributes do not influence the preference of password-based authentication.

Table 6: Model Summary: The perception towards accounts being hacked, biometrics usage, difficulty in storing and setting passwords having a significant impact on the preference between passwordless and password banking.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.429[a]	.184	.171	.456	1.831

a. Predictors: (Constant), Difficulty in Storing passwords, Difficulty in setting passwords as per bank password policy

b. Dependent Variable: Preference between Passwordless and Password banking

R value of 0.487 suggests a moderate positive relationship between the predictors and the preference for passwordless banking. As difficulties with passwords or concerns about security (hacking) increase, the preference for passwordless banking is likely to increase. R Square of 0.237 means that 23.7% of the variance in preference for passwordless banking is explained by the combination of difficulties with passwords, perceptions of security, and use of biometrics.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

A value close to 2, such as 1.872, indicates there is little to no autocorrelation in the residuals, meaning the errors are largely independent.

TABLE 7: ANOVA[a] : The perception towards accounts being hacked, biometrics usage, difficulty in storing and setting passwords having a significant impact on the preference between passwordless and password banking.

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.995	2	2.997	14.424	.000[b]
	Residual	26.600	128	.208		
	Total	32.595	130			

a. Dependent Variable: Preference between Passwordless and Password banking

b. Predictors: (Constant), Difficulty in Storing passwords, Difficulty in setting passwords as per bank password policy

The F-statistic is 14.424, and the p-value (Sig.) is .000, which is highly significant ($p < 0.05$). This means that the model is statistically significant, indicating that the independent variables together predict the dependent variable significantly better than a model with no predictors. Based on the above tables, we can conclude that the relationship between the predictors and the outcome is not due to chance. The analysis shows that the predictors significantly impact the preference for passwordless banking over password banking. Thus, based on the model, there is evidence to conclude that users show a moderate preference towards passwordless banking due to the impact of factors like account security, password management difficulties, and the trust in biometrics.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

CHART 1: Chart showing the common types of passwords less authentication people have come across

Chart 1 reflects the different types of passwordless authentication respondents have come across. The most common is FIDO, experienced by 24.91% of participants, followed by Blockchain Technology at 15.22%. Retinal Authentication at 13.8%, while Cryptographic Passkeys (13.49%) and Decentralised Identity (12.8%) show almost similar levels of familiarity. Magic Link has the lowest exposure, with only 5.8% of respondents having encountered it. There are still 13.8% who have not heard about any of these. This shows the presence of awareness of passwordless authentication methods, indicating room for growth in the broader adoption of these technologies.

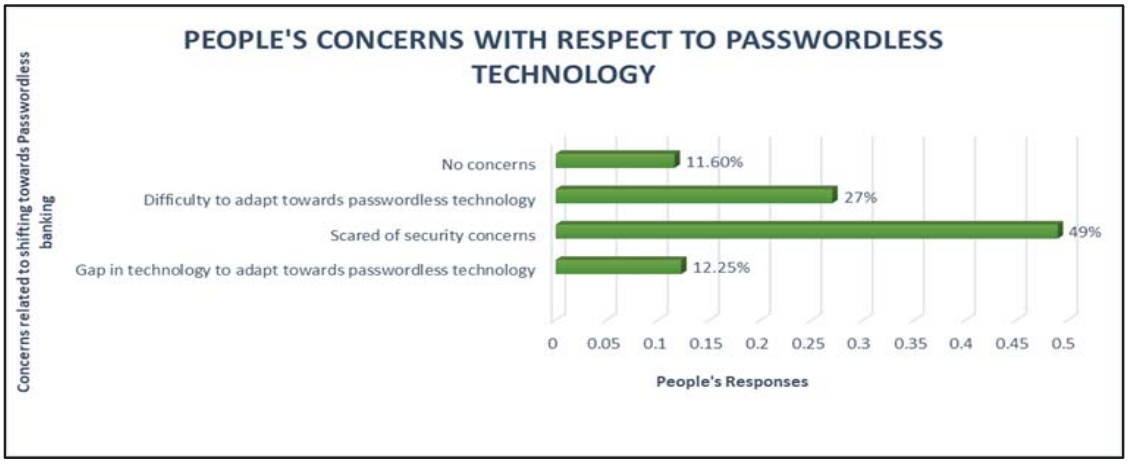

CHART 2: Chart showing people's concerns with respect to passwordless technology

Chart 2 illustrates people's concerns regarding passwordless technology. The biggest concern, at 49%, is security, with respondents feeling unsure about the safety of these methods. Difficulty in adapting to passwordless tech follows at 27%, while 12.25% feel that there is a gap in the technology. Interestingly, 11.6% of respondents expressed no concerns, indicating a level of confidence among some users. This suggests that security concerns remain the main barrier to wider acceptance of passwordless systems.

We can infer from a survey conducted that the consumer behaviour with regards to shifting from the traditional password technology to passwordless technology is highly relative in nature. It reveals that the shift towards passwordless banking is basically governed by the convenience and enhanced security of biometric authentication methods such as fingerprints, facial recognition, OTPs, and token-based systems. The present-day consumers are tech-savvy and are pioneers in leading this shift. From the analysis conducted we observed that there was no association with regards to consumer demographics influencing consumer decisions in adapting and shifting towards passwordless technology. Government regulatory initiatives like Aadhaar-based authentication and UPI have boosted the adoption of passwordless transactions. From the research it was felt that the banking sector needs to reinforce trust by emphasising the safety and security advantages of passwordless systems, data protection and transparency. Overall, while passwordless banking has strong growth potential, addressing challenges such as digital literacy and privacy concerns will be critical for widespread adoption.

CONCLUSION

Passwordless banking technology is the recent development towards shaping the authentication of the banking industry. Passwordless authentication negates the challenges of traditional banking authentication. According to Alex Kreger "Each year technology makes the world more complex for people to understand. So, easy-to- use services for consumers are in particularly great demand." It is hence necessary that the Government takes necessary steps and policies, regulatory supports are enhanced to ensure the smooth transition from password to passwordless technology, leading to a much-secured banking atmosphere by 2047. The concept of Passwordless Banking indeed aligns with the vision of Viksit Bharat@20247 by encouraging both financial inclusion and driving digital transformation.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

BIBLIOGRAPHY

1. Ravilla, Harshavardhan & Kulkarni, Pooja & Sayal, Rishi. (2024). Study and Analysis of FIDO2 Passwordless Web Authentication.
2. Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*, e01743.
3. Yubico and Ponemon, Google, Verizon, Nordpass, FIDO alliance, Gartner, & FIDO alliance. (2023). *Passwordless authentication: The next frontier in security* (p. 04) [Journal-article].
4. Cybersecurity Insiders, HYPR, & Schulze, H. (2021). The state of passwordless security. In *The State of Passwordless Security* [Report]. Cybersecurity Insiders.
5. Singh, H. (2023, March 18). How digitization is shaping the future of banking. *Times of India Blog*.
6. Sengupta, A., & Bfsi, E. (2023, May 5). Will passkeys make BFSI passwordless? *ETBFSI.com*.
7. Guest. (2024, March 9). Revolutionising authentication in India's digital economy. *Financial Express*.
8. *Banking in India: Growth, trends, and opportunities | IBEF*. (n.d.). India Brand Equity Foundation.
9. Martinez, P., & Martinez, P. (2023, January 16). *The Evolution of Digital Banking Authentication – Part 1*. Thales Blog.
10. BIO-key International, Inc. (2024, April 24). *Beyond Passwords: Exploring the Advantages of Passwordless MFA*.
11. *Passwordless Authentication: industry trends*. (n.d.). Passwordless Authentication: Industry Trends.