

Cybersecurity in Digital-Only Banks; How Entrepreneurs Are Shaping India's Digital Finance Ecosystem

Dr. Kamal Agal^{1*}, Dr. Pareshkumar Ukabhai Mordhara², Dr Dharak Patel³, Hetal Rathod⁴, Rohit Khandelwal⁵, Nisha Kadacha⁶

¹Associate Professor, GTU School of Management Studies (GSMS) Faculty of Management, Gujarat Technological University, Ahmedabad, Gujarat (India),

Email ID : asso_kamal@gtu.edu.in

²Assistant professor, B. J. Vanijya Mahavidyalaya (Autonomous), Vallabh Vidyanagar, Anand, Gujarat Email ID : pmordhara@gmail.com

³Assistant Professor, Government Science College, Gandhinagar, Gujarat university, Email ID : dharak.dsp@gmail.com

⁴Assistant professor, GTU School of Management Studies (GSMS) Faculty of Management, Gujarat Technological University, Ahmedabad, Gujarat (India), Email : ap_hetal@gtu.edu.in

⁵Student- MBA (Fintech) GTU School of Management Studies (GSMS), Gujarat Technological University, Ahmedabad, Gujarat (India)

⁶Student- MBA (Fintech) GTU School of Management Studies (GSMS), Gujarat Technological University, Ahmedabad, Gujarat (India)

Corresponding Author:

Dr. Kamal Agal

Associate Professor, GTU School of Management Studies (GSMS) Faculty of Management, Gujarat Technological University, Ahmedabad, Gujarat (India),

Email ID : asso_kamal@gtu.edu.in

ABSTRACT

India's financial landscape is undergoing a radical transformation driven by digital-only banks and fintech innovators. By leveraging Digital Public Infrastructure (DPI) and the "India Stack," these entities provide accessible, simplified, and high-speed banking services to millions. However, this rapid transition has expanded the attack surface, exposing the ecosystem to sophisticated threats such as AI-driven phishing, ransomware, and identity-centric frauds. As India moves toward a digital economy projected to contribute 20% of its GDP by 2026, the intersection of cybersecurity and user trust has become the primary frontier for financial stability. This case study investigates the application of advanced cybersecurity frameworks—specifically Zero-Trust Architecture (ZTA), multi-factor authentication (MFA), and AI-powered threat detection—within the digital-only banking environment. It highlights the pivotal role of entrepreneurs and innovators who are moving beyond mere regulatory compliance to foster a "secure-by-design" philosophy. These leaders are integrating behavioral analytics and end-to-end encryption to safeguard the 48.5% share of global real-time payments that India now commands.

Furthermore, the study incorporates user surveys and case studies (including data from 2024–2025) to analyze consumer behavior and awareness. Findings indicate that while trust in digital platforms is rising, a significant "awareness gap" remains regarding personal cyber hygiene. The research concludes that the sustainability of India's digital finance ecosystem depends on a collaborative model where entrepreneurs, regulators like the RBI, and consumers work in tandem to build a transparent, resilient, and fraud-resistant financial future..

Keywords: Cybersecurity digital, entrepreneurs, Banks, Finance.

.

1. INTRODUCTION:

This case study is about cybersecurity solutions in digital – only banks , with a focus on how digital banks are handling digital payments and all with the help of cybersecurity. Digital banks have grown very rapidly in few years especially after the launch of UPI (unified payments interface) which was launched by NPCI (national payments corporation of India) that allows us to instantly transfer money between bank accounts using a mobile device. There are many apps that provide digital payments services like google pay, Mobi Kwik, fi money, Jupiter, Paytm, phone pay, open, chqbook, fampay &

more. The growth of digital banks was seen during or after covid, due to banned on using 500 & 1000 notes. Peoples were having no other source for payments except for using digital platforms. As a result, the use of Digital Banking was growing rapidly but with the increase in growth it also created many risks related to data safety, privacy, scams, and online frauds and also many digital banks were not given banking license by the government to prevent public data privacy get leaked. The study looks on one of the cases that is Google Pay case, where questions were raised about data privacy and not following rules of The Reserve Bank of India (RBI) and NPCI (National Payments Corporations of India). This shows that cybersecurity is

not only about technology but also about following laws and being transparent with others .To make case study more practical, a questionnaire was also prepared to know how users felt about digital banking. The findings help reveal both the progress and the pitfalls of India's growing digital banking revolution.

Key concepts of the study

What is Cybersecurity?

Cybersecurity in digital banking involves using technologies and strategies to protect financial systems, customer data, and online accounts from unauthorized access, theft, or damage.

Common Cyber Threats:

Malware: - harmful software that damages systems or steals data or unauthorized access without the permission of the user.

Phishing: - fake emails, calls, messages that trick people that they won or received money, now only they need to share OTPs or Passwords.

Data Breaches: - when sensitive data is stolen or leaked.

What are digital banks?

Digital Banks are alike normal banks as it allows peoples to opens accounts, accept payments, transfer money, and also let them to access financial services through online. Digital Banks are also known as neo banks, theses banks have no physical existence they are digitally present. They perform their functions by come into a partnership with banks.

Examples: Jupiter, Paytm, google pay, open and etc.

Key Features:

- 24x7 accessibility
- Paperless transactions
- AI-based customer support
- Low operational costs
- Focus on financial inclusion

Who are entrepreneurs?

Entrepreneurs in your case study are the people who had started digital only banks. They are the one who have the idea to build a bank which functions digitally, entrepreneurs are the visionaries who have seen an opportunity to make banks process easier, faster and more convenient.

Examples:

Vijay Shekhar Sharma founder of Paytm,

Sachin Bansal founder of Navi technologies.

Role of Entrepreneurs in digital banks.

Build more securities.

Invest more in tech field.

Satisfy users by building trust.

Follow all rules and regulations by RBI and NPCI.

Make digital methods of payments easier and more convenient by providing financial knowledge.

The Interconnection Between Entrepreneurship and Cybersecurity

Entrepreneurs help in expanding digital banks by providing finance and there business knowledge and entrepreneurs helps these digital banks by investing in cybersecurity

And also by inventing apps or software who help to detect scams.



(Relationship between digital Banks, Cybersecurity and Entrepreneurs)

CASE STUDY on Digital Banking Security: GOOGLE PAY

INTRODUCTION

Google pay commonly known as google pay is a digital platform for payments developed by google, it allows users to make fast, secure, convenient transactions from any place directly by using their smartphones. It works on UPI (unified payments interference) system in India, it allows instant money transfer from one account to another account without the need of account details. Google pay allows its users to pay bills, allows mobiles recharges and DTH recharges and also gives rewards for doing payments.

Google pay was launched as Tez by google on 18th September 2017 in India. But later in august 2018, Tez was rebranded as google pay globally. Within about a month after launch of Tez (i.e. 18th September 2017) in India the app got approx. 8.5 million downloads & over 30 million transactions by end of October 2017 (just within 37 days after launch). By January 2019, the app (google pay) had reached 100 million installs on the play store in India. Later, in September 2021, the “new” google pay (as it got expanded) crossed over 500 million downloads on the play store. Gpay was mostly installed or used by young smartphones users, peoples who shifted to google pay because of rewards or cashbacks, even Kirana stores, vegetable/fruits vendors.

Setup process of google pay (Google Pay)

Download google pay from play store.

Verify mobile number which is linked with your bank account.

Verification via OTP. (two-factor authentication, cybersecurity is applied here)

Bank account is linked with UPI.

A UPI pin just like ATM pin is created for secure transaction. (UPI pin is an encryption, cybersecurity is applied here too)

Ready to make secure transactions.

Cybersecurity is applied at multiple levels here — OTP verification, encryption of UPI PIN, and two-factor authentication ensure that every payment remains safe and traceable.

Cybersecurity Incidents Related to Google Pay

Like many other Digital Payment platforms or banks, google pay had also faced many cyber security problems like phishing, frauds, and unauthorized transactions. These problems highlight the importance of cyber security in digital world. Few incidents are discussed in this case but there are many. Digital problems not destroys a person financially but even mentally. Let's discuss few incidents of frauds that took place with google pay users.

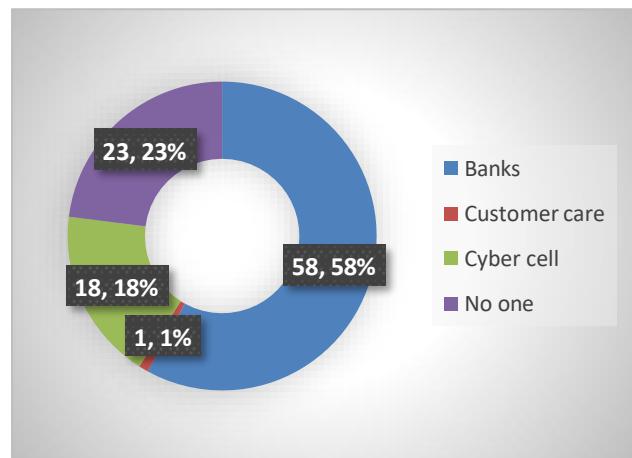
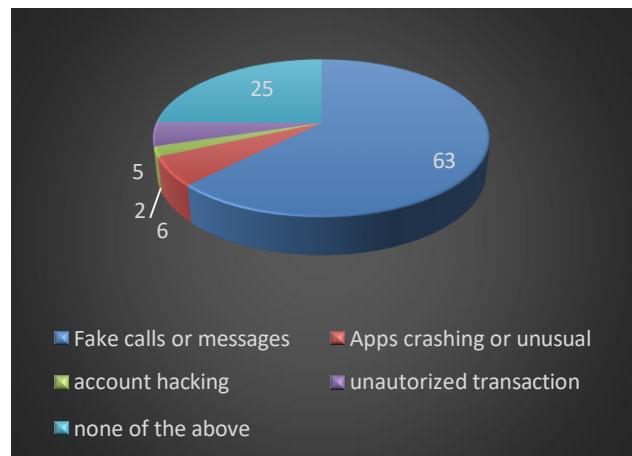


(Payment App Google Pay)

INCIDENT 1 :- Ahmedabad businessman loses nearly ₹3.25 lakh, claims Google Pay got hacked. A businessman named **Uvish Bhardwaj**, a resident of Paldi and owner of Uma Flooring Tiles Company, stated that between 9.57 pm and 10.05 pm on 5 August, an unknown persons gained access to his mobile phone and carried out transactions without requiring an OTP (one-time password). The FIR was registered at Paldi Police Station on 29 August, the hacker made a series of withdrawals totalling an amount of rs.3.249 lakhs from Bhardwaj's linked bank of Baroda accounts, he also claimed that he was not using his app during these transactions, even he also mentioned that he did not received any OTP to share. He said that his phone was hacked and the fraud person misused his google pay app and made such transactions. He visited his banks for the same and found out that there were many payments done from his accounts. He registered complain was forwarded to cyber cell.

Lesson: Cybercriminals can exploit system loopholes or device vulnerabilities, proving the need for multi-layered security and user awareness.

QUESTIONNAIRE RELATED TO THIS INCIDENT



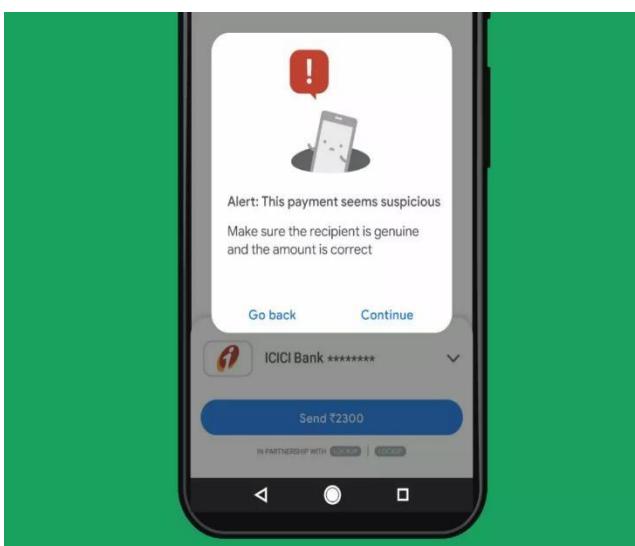
(DIGITAL PAYMENTS FRAUDS) vs (FIRST CONTACT AFTER FRAUD)

INCIDENT 2: - Hyderabad women was gently convinced by a scammer to use google pay & got scammed for Rs.1.7 lakhs. On 19th November 2024, A women got a WhatsApp message from an unidentified number starting with 1-435 claiming that he is his boss. The fraud requested her that he is need of money urgently, at first the victim transferred him a certain amount but after a half an hour, The scammer again messaged her that his UPI id is not working and he needs Rs.1,70,000 for business purpose and promised her that he will pay the whole amount by next morning. But after talking with her boss she found out it was not his boss and she has got scammed. She filled a complain at cybercrime and found out that his boss's phone was got hacked and the investigation is underway.

QUESTIONNAIRE RELATED TO THIS INCIDENT



(Response Towards Small Digital Incidents) vs
(% of Cyber Crime in India)

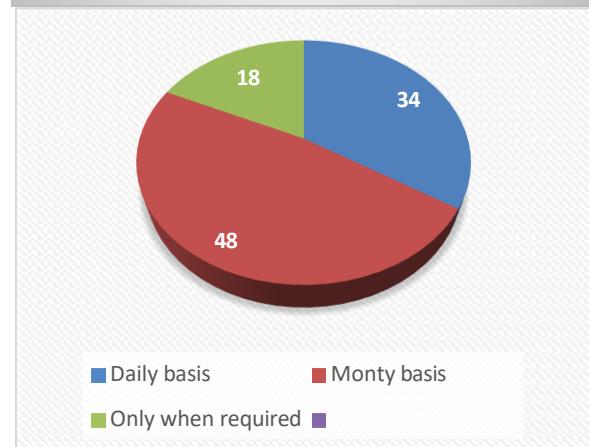
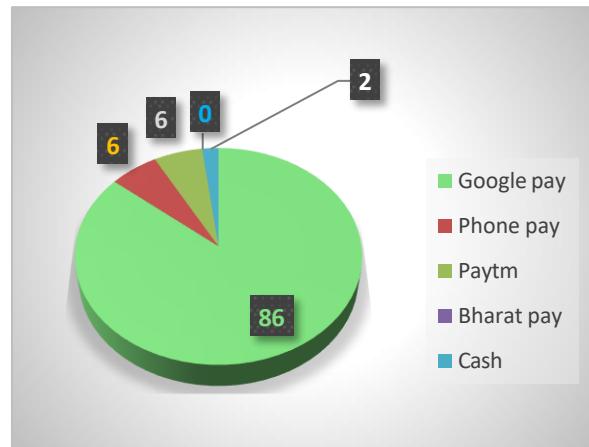


(ALERTS BEFORE ANY SUSPICIOUS PAYEMENTS)

INCIDENT 3 :- New big fraud in Kerala; Beware of accepting money through G Pay, UPI apps. Most business accepts payments through digital platform such as Gpay, Phone pay, Bharat pay, Paytm, & etc. but, nowadays there are many fake apps or counterfeit apps in the market. After purchasing of goods scammers pay amount using fake apps and show screenshot that payments have been done and vendors accepts that as it is same as other payments apps. If it is rush time then vendors just confirm by seeing screenshot of payment

done. As a results vendor faces a loss. Kerala police are trying their best to spread this fake apps among vendors.

QUESTIONNAIRE RELATED TO THIS INCIDENT



(Responses About Use of Payments Apps) vs
(Responses Often Use of Payments Apps)



(FAKE PAYEMNTS APPS IN INDIA)

INCIDENT 4:- Paytm accuses Google Pay of sharing data with group companies and third parties. In 2018, Paytm accused Google Pay of mishandling Indian users' payments data. Google Pay was sharing customer data with its group companies (other than Google) and third-party service providers. User transaction data was being used for advertisements and promotions. Payment's data was being stored outside India, violating RBI's data-localization rules. The reserve bank of India (RBI) gave warning to all digital banks that public data should be

stored in India only. Google denied all such allegations and said they do not share or use customer data for advertisement, promotion, and etc. they share data only with authorized partners (banks, billers, merchants) to carry or process transactions. Google was not legally charged. As google pay prove that they follow all types of rules and policies set by RBI or NPCI.

Google Pay vs Paytm COMPARISON ON DATA PRIVACY		
	Some data stored outside India	Data stored entirely in India
	Shares data with authorized partners	No third-party data sharing
	Initially disputed; later complied	Fully compliant
	Medium	High
Public Transparency	Medium	High



(CLASH BETWEEN PAYTM AND GPAY)

INCIDENT 5: - Google flags 4.1 crore transactions on GPay, blocks 60 million risky app installs. On 17th June 2025, Google said that they had warned more than 4.1 crore Indian users on UPI, Google pay , Paytm against suspicious transaction. Google said that they had built AI powered fraud detector system, it can recognise any fraud events such as fraud message, phone calls, anti-money laundry. This system was built as digital payments are growing rapidly in India with a effect of growing digital scams. At the same time, its Android security system blocked around 60 million risky app installs globally, many of which could have been used for financial fraud, phishing, or stealing sensitive information like SMS OTPs. Google also introduced google play protect so it detects frauds before installing any app. Google introduced **DigiKavach**. It is a program by Google in India focused on online fraud identification. It studies how scammers operate, works with partners (Fintech, consumer groups), builds awareness and implements protections against emerging digital financial scam. It

helps to protect Google Pay users by identifying new scams. These new software's saves users' data, prevent privacy and also users are now known in advance that it can be a scam message, scam calls, scam OTP & many others scams were now easy to detect.



(APPS INDIRECTLY ACCESS PAYMENTS APPS)

The main objectives of this case study are:

To understand the use of digital platforms.

To understand the meaning of digital banks and cybersecurity.

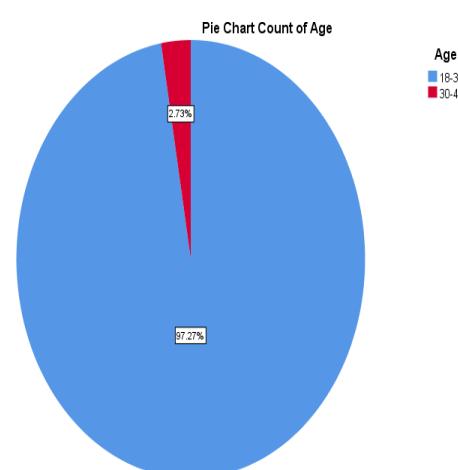
To understand the different incidents took place with google pay.

To understand the common digital problems in India.

To understand the cybersecurity solutions for digital problems.

To understand the role of entrepreneurs in digital banks.

QUESTIONNAIRE RESPONSES ANALISATION AND INTERPRETATION



(AGE GROUPS)

Frequency Table

How you make payments ?

	Frequency	Percent	Valid Percent	Cumulative Percent
Advances in Consumer Research				

Valid	Both	36	32.7	32.7	32.7
	Cash	3	2.7	2.7	35.5
	Online	71	64.5	64.5	100.0
	Total	110	100.0	100.0	

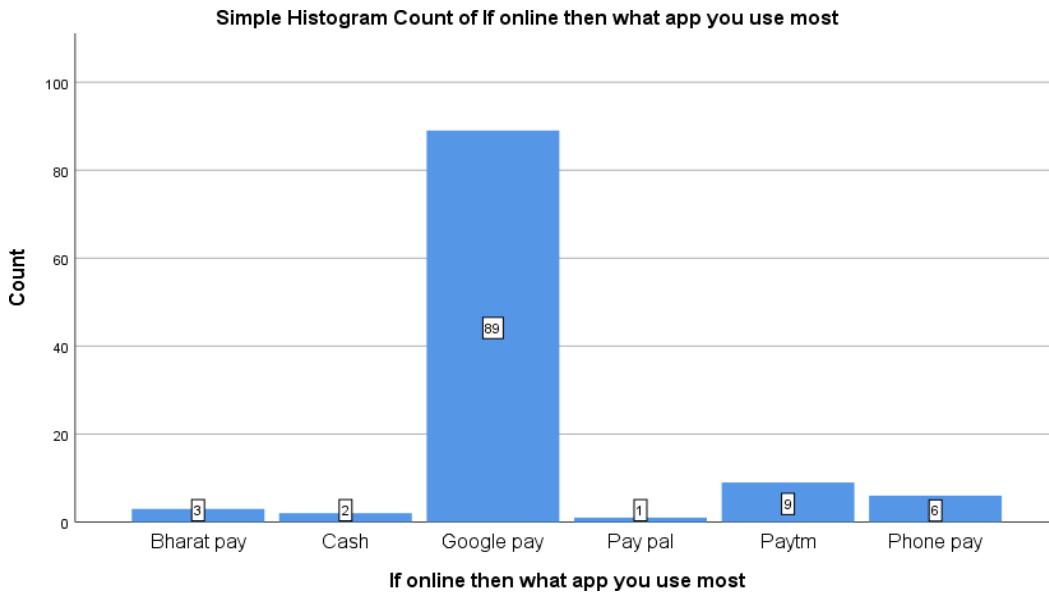


Figure 1 Usage and Awareness of Online Payments

INTERPRETATION

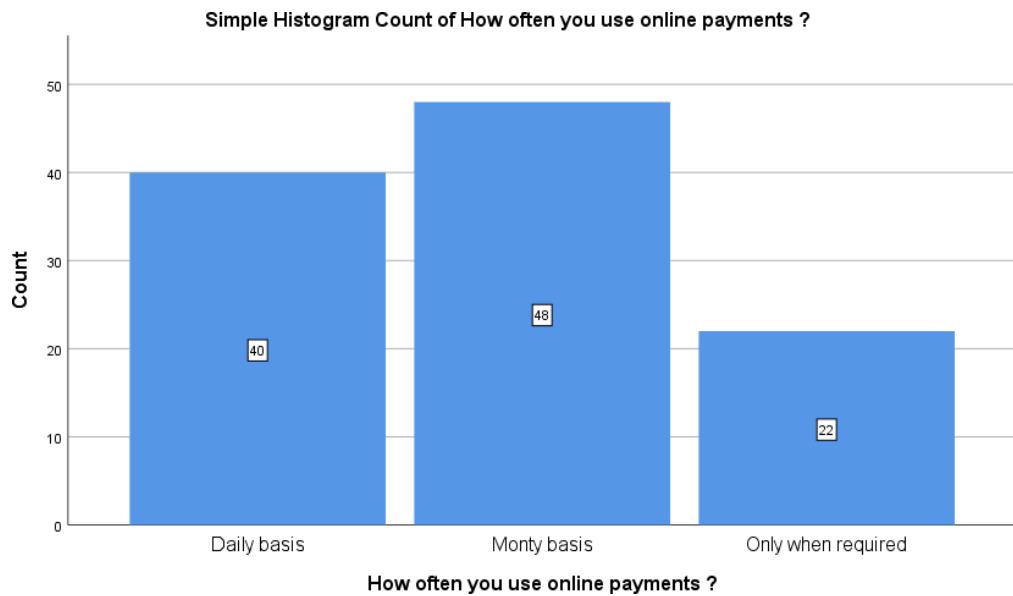
Most respondents are **18–30 years old**, showing young users prefer digital payments. About **64.5% use online methods**, and **Google Pay** is the most popular app. This means **digital payments are widely accepted among youth**, mainly because they're **fast, easy, and secure**.

Frequency Table

How often you use online payments ?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daily basis	40	36.4	36.4	36.4
	Monty basis	48	43.6	43.6	80.0
	Only when required	22	20.0	20.0	100.0
	Total	110	100.0	100.0	

Are you aware of the importance of setting a strong password or pin for your digital payment apps.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	1	.9	.9	.9
	Yes	109	99.1	99.1	100.0

	Total	110	100.0	100.0	
--	-------	-----	-------	-------	--



Security Perception and Issues in Digital Payments

INTERPRETATION

The results show that most people use online payments either monthly or daily, which means digital transactions have become a common habit. Only a few use them only when needed. This shows that people are now more and more using online payment apps in their day to day life.

Almost everyone in the survey mentioned that they know the importance of keeping a strong password or PIN, which shows users are getting aware of how to protect their accounts and use digital payments..

Frequency Table

Do you think two factor authentication is good or not ?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	May be	8	7.3	7.3	7.3
	No	1	.9	.9	8.2
	Yes	101	91.8	91.8	100.0
	Total	110	100.0	100.0	
Do you think you are safe when you use digital payments ?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	May be	30	27.3	27.3	27.3
	No	12	10.9	10.9	38.2
	Yes	68	61.8	61.8	100.0
	Total	110	100.0	100.0	

Have you ever experienced any of the following issues while using digital payments ?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Account hacking	2	1.8	1.8	1.8
	Apps crashing or unusual behaviour	6	5.5	5.5	7.3
	Fake calls or messages	67	60.9	60.9	68.2
	None of the above	30	27.3	27.3	95.5
	Unauthorised transaction	5	4.5	4.5	100.0
	Total	110	100.0	100.0	

Pie Chart Count of Have you ever experienced any of the following issues while using digital payments ?

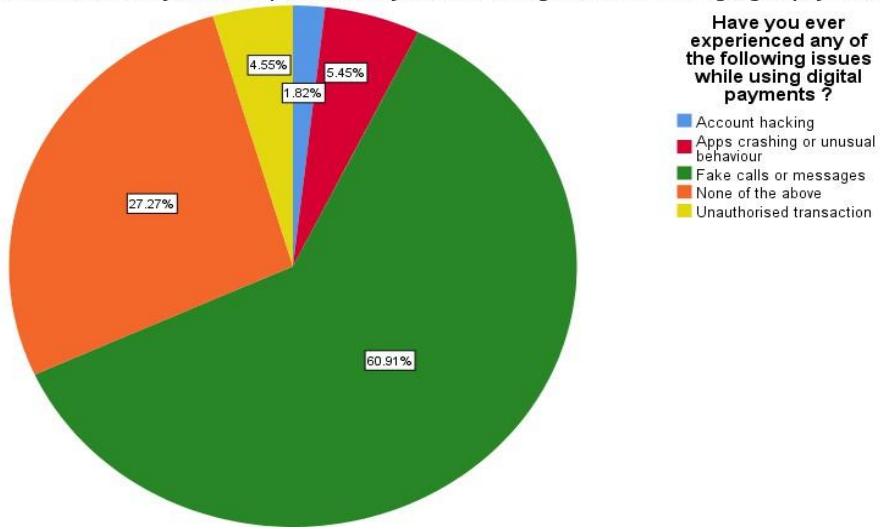


Figure 2 Payment Methods and App Preferences

INTERPRETATION

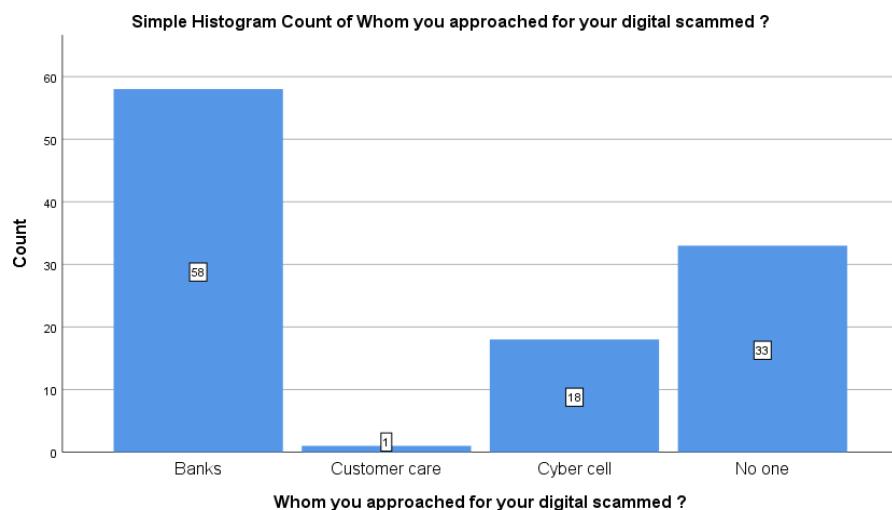
Most respondents have experienced fake calls or messages, which shows that scammers try to reach out public usually through calling or messaging as this way they are able to get customers details. The analysis shows

also that very few respondents were got hacked, so this shows that people are using multi factor authentication or are aware of multi factor authentication. Almost 30% of respondent's does not face any digital payments issues which is sign of digital awareness which is comparatively less as compare to respondent's who thinks that they are safe while using digital payments.

Frequency Table

Respondents' responses related to role of cyber security in digital banks.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	NO	14	12.7	12.7	12.7
	Yes	96	87.3	87.3	100.0
	Total	110	100.0	100.0	

Whom you approached when u face digital scams ?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Banks	58	52.7	52.7	52.7
	Customer care	1	.9	.9	53.6
	Cyber cell	18	16.4	16.4	70.0
	No one	33	30.0	30.0	100.0
	Total	110	100.0	100.0	



Role of Cybersecurity in Digital Banking

INTERPRETATION

Almost 88 % respondent's says that in digital banks cybersecurity have a very main and important role, which shows that people knows the importance of data privacy and security.

But usually during any digital scammed people visits banks for the solutions , over half (52.7%) feels the same way . even 30% of people have not visited anyone during digital scams which shows that many users still have less awareness of where to report online frauds or they think it will be bad for their image to report such scams .

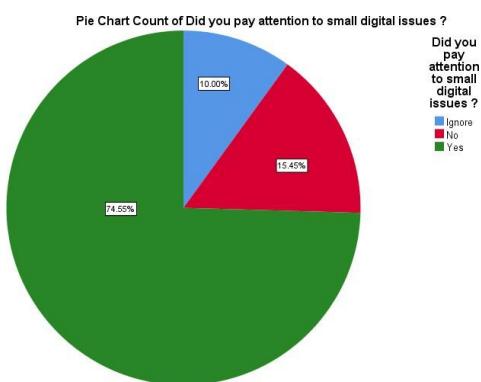


Figure 3 Payment Methods and App Preferences

INTERPRETATION

The analysis shows that most of the respondents are aware of the digital issues as they pay attention even on their small digital problem.approx 75% people thinks that they should be actively aware of small digital problems. A smaller portion, 15.45%, responded "No", suggesting they do not pay much attention to such issues. Only 10% chose "Ignore", indicating a few people deliberately overlook small digital problems.

Overall, the chart suggests that most respondents are attentive to small digital issues, while a smaller number either overlook or ignore them.

ROLE OF ENTREPRENEURS IN ALL INCIDENTS

Entrepreneurs can develop AI powered fraud detection system similar to what google had developed to identify fraud and block such activities.

Entrepreneurs can collaborate with FINTECH companies.

Entrepreneurs can launch program system like DIGIKAVACH for users.

Entrepreneurs can help digital banks to secure public data & stored that data as per jurisdiction of India and help to share such data only with authorized entities.

Entrepreneurs can conduct financial literacy programs or workshops or demo lectures to educate more people about financial terms and digital payment platforms.

Entrepreneurs can help in development or they can develop apps that help public to know whether the payment app used by the customer or payer is not a fake app.

Entrepreneurs can invest more money in fintech or digital or neo banks as they used to face losses due to less capitals or their capital is utilized in problem solving rather than developing technology.

Entrepreneurs can Design banking products and support services that are accessible to low-literacy and rural populations, with simplified UIs, local language options, and voice-based assistance.



(ENTREPRENEURS INVESTMENTS IN DIGITAL WORLD PAYMENTS)

2. CONCLUSION

Entrepreneurs act as the bridge between technology and trust. Their decision for investing in digital protection software determines that whether banking systems remains innovative and secured too. This can be achieved by transparent business practises . entrepreneurs helps in developing and shaping digital finance.



(ENTREPRENEURS ROLES IN DIFFERENT WAYS)

COMMON DIGITAL BANKING PROBLEMS

Despite rapid growth that is happening in digital banking sector, many users continue to face challenges related to **security, trust, and awareness**. These issues can lead to financial losses, stress, and hesitation in adopting digital payments. The most common digital banking problems are given below: -

1. Hacking

Most of the times people's phones usually get hacked & they face fraud payments.

2. Fake Messages

Unidentified messages are one of the causes for frauds. Scammers messages users by Impersonate themselves as user's friends, relatives, families, colleges, and even their superior.

3. Fake Apps

Fakes and Counterfeit Apps are the most important emerging problem in digital world specially in digital banks and their main targets are usually small vendors.

4. Data Leak Risk

In some cases, it is found that digital payments apps share their user's data with third parties without their concern, in case of Paytm.

5. Unauthorized Data Access

Now a days there are many others apps which are not digital banks apps but they are able to access users' financial data.

6. Fake Lottery Scams

Most of the time people are getting scammed because they became the direct target by providing their accounts details, in case of winning fake lottery or Jackpots.

7. Fake Adds

Fake adds are also one of the common reasons for digital scams.

8. Urgent Need Fraud

One of the reasons behind digital scam is urgency, people in urgency provide their details to unknown persons.



3. CONCLUSION

This concludes that cyber security has many problems to handle and deal with them. These common problems are not only face by poor or middle-income people but also rich ones. these digital problems are common in India and are increasing on a very high phase.

Technology itself cannot ensure the safety of users; users themselves must also stay alert and adopt responsible digital prevention habits. Governments, Banks, and Fintech Entrepreneurs should work together to build Transparent and secured digital platform for payments and also promote financial literacy. Only through a combined effort of innovation and awareness can Digital banking in India become both secure and inclusive for everyone.

CYBER SECURITY SOLUTIONS FOR ALL INCIDENTS

In the fields of digital only banks cybersecurity plays a very important role as it prevents scams and frauds by **advanced technology, strict regulation, and public awareness** to create a truly secure digital environment.

Here are the key **cybersecurity solutions** that can help address common digital banking incidents:

1. Multi-Factor Authentication (MFA)

Cyber security can build multi factor Authentication for login. Cyber security can develop more layers of safety for digital payments. Use of biometric authentication (face or fingerprint) to carry out all types of transaction.

2. Real-Time Fraud Detection using AI

Cyber security can implement machine learning algorithms to dynamically update threat profiles. Cyber security can scan & block fake apps before they reach end users.

3. Secure Payment Verifications

Cyber security can make apps that can help to identify that payment has been receipts rather than trusting on a screenshot.

4. Provide Awareness About Scams

Cyber security can educate public about common frauds such as OTP scams, Counterfeit apps & more. Cyber security should literate public about fake messages, calls and delivery OTP's.

5. Auditing And Verifying

Cyber security should continuously audit & verify digital transactions of vendors, partners, and third-party service providers.

6. Following RBI Guidelines

Cyber security should work as per RBI guidelines about how users should use digital banking apps.

7. End-To-End Encryption

Cyber security should apply privacy-by-design and secure coding standards during the creation of digital bank services, minimizing risk exposure from the ground up.



(7 PILLARS OF CYBERSECURITY) CONCLUSION

Cybersecurity is not just a technical necessity — it's the foundation of trust in digital banking. Combining strong authentication, AI-based monitoring, compliance with RBI regulations, and public awareness ensures a safe and transparent financial ecosystem. As India moves closer to a cashless future, cybersecurity will remain the key to sustaining that progress.

responsibly.

CONCLUSION OF THE CASE

From the case study, it is concluded that without cybersecurity digital banks have no digital existence in the market as without cybersecurity public won't trust any digital banks as their privacy and data are at risk. Cybersecurity acts like a shield it detects attacks, blocks hackers, and keeps sensitive details (like account numbers or passwords) safe. It ensures that personal data stays private and isn't misused. But sometimes even if there is cybersecurity people should not blindly trust on apps for digital payments. people should always do research before using any banking app

As in case if that app is not reliable then it can cause harm to privacy of public.

This case also concludes that people should always double check before believing on any calls, messages, and links. Without cybersecurity, banks become easy targets for fraud, identity theft, and data leaks. Customers would lose trust, financial losses would rise, and the entire digital banking system could collapse. From the case study we can say that entrepreneurs are important part of digital Banking. Entrepreneurs bring innovation by creating new apps, security solutions, and business models that strengthen digital banking. Their fresh ideas help banks stay ahead of hackers while making banking easier and safer for people.

REFERENCES

1. Banerjee, T., & Nair, S. (2024). The cybersecurity conundrum: Unravelling UPI scams in India. *International Journal of Research in Engineering and Applied Sciences*, 14(2), 75–86. https://euroasiapub.org/wp-content/uploads/IJREAS5Feb2024_V.pdf
2. Business Standard. (2017, March 16). India to promote indigenous expertise in cyber security, fund start ups. *Business Standard*. https://www.business-standard.com/article/companies/india-to-promote-indigenous-expertise-in-cyber-security-to-fund-start-ups-117031600030_1.html
3. Chatterjee, S., & Mohanty, A. (2024). Digital transformation in the Indian banking sector: Opportunities, risks and regulatory responses. *SSRN Electronic Journal*. <https://papers.ssrn.com/sol3/Delivery.cfm/4987052.pdf>
4. Data Security Council of India. (2025). India cyber threat report 2025. *DSCI*. <https://www.dsci.in/resource/content/india-cyber-threat-report-2025>
5. Desai, K., & Verma, N. (2023). Digital payments are secure or not: A study of users' perception in India. *International Research Journal of Modernization in Engineering, Technology and Science*, 5(11), 900–908. https://www.irjmets.com/upload_newfiles/irjmets7110041767/paper_file/irjmets71100041767.pdf
6. Deshkar, A. (2025, March 28). P2P scams: How they can drain your money through UPI in just seconds. *The Indian Express*. <https://indianexpress.com/article/technology/tech-news-technology/p2p-scams-how-they-can-drain-your-money-through-upi-in-just-seconds-9911184/>
7. Drishti IAS. (2025, February 11). India to become a fintech powerhouse. *Drishti IAS*. <https://www.drishtiias.com/daily-updates/daily-news-editorials/india-to-become-a-fintech-powerhouse>
8. Enterslice. (2023, February 28). Cybersecurity in digital banking: Threats, challenges & solutions. *Enterslice*. <https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challenges-and-solution/>
9. GIMS Business School. (2025, November 18). *FinTech in India: Growth, trends and the future of digital finance*. *GNIOT Institute of Management Studies*. <https://www.gims.net.in/blog/2025/11/18/fintech-in-india-the-new-frontier-of-finance/>
10. Gujarat Samachar. (2025, August 30). Ahmedabad businessman loses nearly ₹3.25 lakh, claims Google Pay got hacked. *Gujarat Samachar*. <https://english.gujaratsamachar.com/news/gujarat/ahmedabad-businessman-loses-nearly-3-25-lakh-claims-google-pay-got-hacked>
11. Gupta, A., & Mehta, S. (2025). Growth of UPI transactions in India: A digital revolution in payments. *International Journal of Science and Research*, 14(6), 120–128. <https://www.ijsr.net/getabstract.php?paperid=SR25604195127>
12. Indian Institute of Banking & Finance. (2025). Cyber risk management in Indian banks. *Bank Quest*, January–March. <https://www.iibf.org.in/documents/BankQuest/2025/January-April%202025/Bank%20Quest%20-%20January%20to%20March%20issue.pdf>
13. Jose, A., & Nair, S. (2023). The impact of cybersecurity awareness on customers' trust and adoption of internet banking in Palakkad district. *International Journal of Innovative Research in Technology*. https://ijirt.org/publishedpaper/IJIRT179242_PAPER.pdf
14. Joshi, P., & Rao, R. (2023). A survey on digital payment system in India. *International Journal of Management, Science, and Technology Research*, 3(4), 55–63. <https://www.ijmsrt.com/storages/download-paper/IJMSRT25MAY091>
15. Joshi, R., & Varma, P. (2025). Trust and cybersecurity in digital payment adoption: Socioeconomic determinants in India. *Journal of Banking and Socioeconomic Development*. <https://www.emerald.com/jbsed/article/doi/10.1108/JBSED-04-2025-0119/1268531/Trust-and-cybersecurity-in-digital-payment>
16. Kaur, M., & co authors. (2024). FinTech entrepreneurial ecosystem in India: Role of policy, funding and innovation hubs. *Accounting & Finance*. <https://www.sciencedirect.com/science/article/abs/pii/S104402832400005X>
17. Kerala Kaumudi. (2025, May 20). New big fraud in Kerala; Beware of accepting money through G Pay, UPI apps. *Kerala Kaumudi*. <https://keralakaumudi.com/en/news/news.php?id=1537>

481&u=new-big-fraud-in-kerala-beware-of-accepting-money-through-g-pay-upi-apps

18. Khan, M., & Reddy, L. (2023). Cyber security models in the banking sector in India and their effectiveness. *International Journal of Novel Research and Development*, 8(6), 210–218. <https://ijrnd.org/papers/IJNRD2306478.pdf>

19. Khan, S., & Desai, V. (2025). An analytical study on cybersecurity threats in the Indian banking sector. *International Journal of Research Publication and Reviews*, 6(6), 450–459. <https://ijrpr.com/uploads/V6ISSUE6/IJRPR48431.pdf>

20. KnowledgeHut. (2025, April 27). Cybersecurity in banking: Importance, threats, challenges. KnowledgeHut. <https://www.knowledgehut.com/blog/security/cyber-security-in-banking>

21. Kumari, N., & Singh, R. (2025). Digital transformation in India's banking industry: Opportunities, challenges and cyber security concerns. *Young Researcher*. <https://rya.ijaar.co.in/wp-content/uploads/2025/02/S140124.pdf>

22. Kumar, P., & co authors. (2021, August 1). Scoping the need of mainstreaming Indigenous Knowledge Systems for sustainable development and societal resilience. *Journal of Ethnobiology and Ethnomedicine*, 17(1). <https://pmc.ncbi.nlm.nih.gov/articles/PMC8327904/>

23. Kumar, R., & Singh, P. (2024). Revitalizing Indigenous Knowledge System: Strategies and challenges under NEP 2020. *International Journal of Humanities and Social Science Management*. https://ijhsm.org/issue_dcp/Revitalizing%20Indigenous%20Knowledge%20System%20Strategies%20and%20Challenges%20under%20NEP%202020

24. Lathwal, S. (2024). Integration of Indian Indigenous Knowledge System in management: Prospects and challenges. *International Journal of Trend in Scientific Research and Development*. <https://www.ijtsrd.com/papers/ijtsrd63500.pdf>

25. Ministry of Electronics and IT. (2025). India cyber threat landscape and indigenous security solutions. In *India cyber threat report 2025*. Data Security Council of India. <https://www.dsci.in/resource/content/india-cyber-threat-report-2025>

26. Ministry of Finance, Department of Financial Services. (2019, August 29). Cyber security and fintech. Government of India. <https://financialservices.gov.in/beta/en/page/csft>

27. Mitigata. (2025, September 28). Cyber insurance for fintech in 2025: Essential coverage. Mitigata. <https://mitigata.com/blog/cyber-insurance-for-fintech/>

28. Mohammed Rayees ur Rahim. (2024, November 19). Hyderabad woman duped of Rs. 1.7 lakh as fraudster posed as her boss. *Hyderabad Mail*. <https://hyderabadmail.com/hyderabad-woman-fraud-google-pay/>

29. Nair, M., & Prasad, K. (2025). Integrating indigenous knowledge systems into modern cyber law and digital ethics. *VIIRJ*. <https://www.viirj.org/specialissues/2025/SP2502/69.pdf>

30. National Cyber Security Coordinator. (2023). Towards a (secure?!) digital nation: Indian ethos, knowledge and cyber resilience. National Critical Infrastructure Protection Centre. <https://nccg.gov.in/assets/pdf/Plenary-2-Towards-Secure-Digital-Nation.pdf>

31. OpenGov Asia. (2025, March 20). India: Digital sovereignty with indigenous web browser. *OpenGov Asia*. <https://archive.opengovasia.com/2025/03/21/india-digital-sovereignty-with-indigenous-web-browser/>

32. Pathak, A., & Mehta, S. (2025). Cybersecurity disruptions in the Indian banking sector and regulatory responses. *Journal of Emerging Technologies and Innovative Research*. <https://www.jetir.org/papers/JETIR2503331.pdf>

33. Patel, N., & Deshmukh, R. (2023). An analytical study on cybersecurity threats in the Indian banking sector in the digital era. *International Journal of Research Publication and Reviews*, 6(6), 450–459. <https://ijrpr.com/uploads/V6ISSUE6/IJRPR48431.pdf>

34. Poyer, A., & co authors. (2023). Indigenous sustainable finance as a research field. *Accounting & Finance*, 63(4), 567–593. <https://onlinelibrary.wiley.com/doi/10.1111/acfi.13062>

35. PwC India. (2020). FinSec: An emerging equation between fintech and cybersecurity. *PricewaterhouseCoopers India*. <https://www.pwc.in/assets/pdfs/fin-sec-an-emerging-equation-between-fin-tech-and-cybersecurity.pdf>

36. Rani, S., & Kumar, V. (2025). A study on neo-banking in India: Growth, challenges and future prospects. *International Journal of Research in Granthaalayah*, 13(8), 45–60. <https://www.granthaalayahpublication.org/journals/granthaalayah/article/download/6328/6255>

37. Rao, A., & Kulkarni, P. (2025). A Neo-Vedic framework for e-banking cybersecurity in the Indian context. *European Journal of Management and Research*, 5(11), 101–115. <https://www.eelet.org.uk/index.php/journal/article/view/3878>

38. Rao, S. K., & Iyer, M. (2024). Digital banking evolution in India: Bridging convenience, security and financial inclusion. *EEELET Journal*. <https://www.eelet.org.uk/index.php/journal/article/download/2465/2218/2727>

39. Reserve Bank of India. (2020). Cyber security framework for urban cooperative banks (UCBs), 2020–2023. Reserve Bank of India.

40. Scroll Staff. (2018, September 21). Paytm accuses Google Pay of sharing data with group companies and third parties. *Scroll.in*. <https://scroll.in/latest/895224/paytm-accuses-google-pay-of-sharing-data-with-group-companies-and-third-parties>

41. Sharma, K., & Reddy, P. (2024, January 30). A study on cyber security threats in digital banking and mitigation strategies. *ShodhKosh: Journal of Visual and Performing Arts*. <https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/view/4924>

42. Sharma, P., & Gupta, A. (2025). A comparative study of cybersecurity challenges in public and private sector e banks in India (2020–2024). *International Journal of Commerce and Management Research*. <https://www.multiarticlesjournal.com/counter/d/4-1-58/IJCRM20254158.pdf>

43. Sharma, P., & Iyer, D. (2024). Neo banking and its impact on the overall banking ecosystem in India. *International Journal of Multidisciplinary Studies and Recent Trends*, 6(5), 35–42. <https://ijrpr.com/uploads/V6ISSUE5/IJRPR46984.pdf>

44. Sharma, R. (2025, July 7). Digital payments vs digital risks: India's fintech ambitions and AI driven security. *The Times of India*. <https://timesofindia.indiatimes.com/business/cybersecurity/digital-payments-vs-digital-risks-indias-fintech-ambitions-and-bridging-the-security-gap/articleshow/111234567.cms>

45. Singh, R., & Sharma, P. (2024). UPI frauds: A study on UPI usage, awareness and impact in India. *International Journal of Research in Commerce and Management Studies*, 6(2), 179–197. https://ijrcms.com/uploads2024/ijrcms_06_312.pdf

46. Sivaraman, R. (2024, April 27). T.N. Cyber Crime Police issue advisory on new scam involving AI voice cloning. *The Hindu*. <https://www.thehindu.com/news/national/tamil-nadu/tn-cyber-crime-police-issue-advisory-on-new-scam-involving-ai-voice-cloning/article68113216.ece>

47. Sengupta, M. (2015). Obstacles to the use of indigenous knowledge. *Economic and Political Weekly*, 50(9), 23–26. <https://www.jstor.org/stable/24565835>

48. Sood, N. (n.d.). Scam alert: Google flags 4.1 crore transactions on GPay, blocks 60 million risky app installs. *Moneycontrol*. <https://www.moneycontrol.com/technology/scam-alert-google-flags-4-1-crore-transactions-on-gpay-blocks-60-million-risky-app-installs-article-13131351.html>

49. Teji Mandi. (2025, October 15). India's fintech industry: Growth, start ups, and outlook. *Teji Mandi*. <https://tejimandi.com/blog/feature-articles/indias-fintech-industry-growth-start-ups-and-outlook>

50. Vasudevan, S., & Rao, K. (2024). Analysis on fraudulent threats and mitigating strategies in UPI transactions. In *Proceedings of the International Finance Conference* (pp. 52–60). <https://www.sdmimd.ac.in/conferenceproceedings/ifc2024papers/IFC2452.pdf>