European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

CYBERSECURITY RISKS AND DATA PRIVACY CONCERNS IN PMJDY DIGITAL TRANSACTIONS

Bharti Kumari
Research Scholar, Department of Commerce,
Shyama Prasad Mukherjee Govt. Degree College, University of Allahabad

Dr. Alok Singh
Assistant Professor, Department of Commerce,
Shyama Prasad Mukherjee Govt. Degree College, University of Allahabad

Abstract

The Pradhan Mantri Jan Dhan Yojana (PMJDY) has significantly improved financial inclusion in India by providing banking access to millions, particularly in rural and low-income communities. With the growing use of digital platforms like Aadhaar-enabled payment systems (AePS), mobile banking, and UPI under PMJDY, financial services have become more accessible and efficient. However, this shift to digital has also introduced serious cybersecurity and data privacy challenges. Many account holders lack digital literacy, making them vulnerable to fraud, including phishing, identity theft, and biometric misuse. Additionally, weak infrastructure, poor device security, and limited user awareness exacerbate the risks. The integration of Aadhaar for financial authentication has raised concerns about data privacy, particularly regarding unauthorized access to data and the lack of clear user consent. This paper investigates these emerging threats, examines relevant legal frameworks such as the Digital Personal Data Protection Act, 2023, and evaluates real-world fraud cases involving PMJDY users. It proposes practical solutions, including stronger security protocols, improved regulatory oversight, and widespread digital literacy initiatives. Ultimately, safeguarding digital financial services is essential to maintaining public trust and ensuring the long-term success of PMJDY's mission of inclusive economic growth.

Keywords: Financial Inclusion, PMJDY, Cybersecurity Risks, Data Privacy, Digital Transactions, Aadhaar-linked Services

Introduction

The Government of India launched the flagship scheme of Pradhan Mantri Jan Dhan Yojana (PMJDY) in 2014 to facilitate financial inclusion. The program was designed to make sure that access to basic banking facilities was provided to all households, particularly in economically and geographically disadvantaged regions. Through the years, the PMJDY has empowered millions of people in opening bank accounts, taking the benefits of government subsidies, and accessing credit and insurance options. The increasing accessibility of bank services made the PMJDY possible, which has been instrumental in empowering the citizens and leading to a more inclusive economic growth by addressing the discrepancy between the formal banking institutions and the underserved population segments.[1]

As more technologies become incorporated in the Indian financial system, the provision of PMJDY services is now drastically moving to the digital platforms. Enrolment-linked bank accounts, mobile, RuPay debit cards, and a unified payment interface (UPI), visions have become part of the functioning of Aadhaar in the scheme. This change has, without a doubt, made the system more efficient and wider in terms of coverage and ease of access to the beneficiaries, as well as in the minds of the beneficiaries to access financial aid and assistance in their accounts. But this widespread embrace of the digital space has also brought with it a different and rather alarming series of issues, most specifically those of cybersecurity and data protection.[2]

A large part of the PMJDY beneficiaries comprises members of the society who are less exposed to digital technologies and hardly aware of cyber safety measures. Consequently, they become susceptible to digital scammers like phishing, hacks on their accounts, SIM swapping, and identity theft. With the absence of digital literacy among its users, scammers tend to recruit them by misleading people via false links, scam calls, or false apps. Moreover, there have been various instances in which personal information and financial data have been stolen because of either technological vulnerability or human error.[3]

The aspect of integrating Aadhaar in accessing identities and transactions presents issues on the security of sensitive personal and biometric data. These are past cases that have revealed huge amounts of information that is Aadhaar-related online. The number of people who are not properly informed about their data operations, sharing, or storing suggests the issue of informed consent and privacy. Although there was the Digital Personal Data Protection Act, 2023, there have been irregularities in implementing the standards of data privacy, especially noted in regions where PMJDY has the most beneficiaries. The fact is that rural users do not have access to remedy facilities or details regarding their online rights. Service providers and financial intermediaries conducting transactions via PMJDY may not follow close cybersecurity measures, exposing them to the probability of theft or misuse of information.[4]

Literature Review

The Pradhan Mantri Jan Dhan Yojana (PMJDY) has been considered as one of the radical programs towards the aspect of financial inclusion in India. Researchers have highlighted the ability of the scheme to ensure that the low-income and excluded populations get access to formal banking services (Kapoor & Tyagi, 2020; Singh & Deep, 2025). The extension of its services to the areas of savings, credit, insurance, and direct benefit transfers has helped it to reduce the untouchability of finance and enhance better socio-economic outcomes (Verma & Garg, 2016; Bhardwaj, n.d.).

According to empirical approaches, it seems that PMJDY has already helped to incorporate millions of people into the formal banking system, including high penetration into rural and semi-urban quarters (Ravikumar, 2018; Srivastava, Sharma & Deshpande, 2019). Besides, the effectiveness of Indian banks in the implementation of the scheme has been discussed with the use of DEA approaches that have taken into consideration diverse institutional capabilities in states (Singh & Deep, 2025). Significant regional effects have also been noted through the PMJDY, e.g., among Scheduled Tribes in Kerala, where financial literacy played a factor role in the utility of an account and its awareness (Kurussiveettil & Kanniammal, 2024).

A number of authors have demonstrated that there is a close relationship between digital tools and the success rate of PMJDY (Ramasethu, 2016; Chowhan & Pande, 2014). Under the inclusion of mobile banking, Aadhaar, and UPI, the digital environment has boosted penetration and performance (Malik, 2014; Tripathi, Yadav, and Shastri, 2016). Nevertheless, this digital innovation has also come with its setbacks of cybersecurity issues, as said by Tripathy (2025), who details the increasing frequency of cybercrimes in India in the financial sector in the recent decade.

The increase in online payments has revived the issue of data privacy, particularly when there are Aadhaar-related services. Blockchain has become a possible way out of these difficulties because it can provide a decentralized method of storing data and verifying transactions without violating privacy (Hassan, Rehmani & Chen, 2019; Elisa et al., 2020; Haque & Rahman, 2020). Its applications (including safe e-governance initiatives and repairs of monetary infrastructure) have become the latest technologies that have been suggested.

Research-oriented analyses have provided insights into the design and implementation of PMJDY. It has also been emphasized that the results available so far support the idea that the policy-induced inclusion can result in long-term behavioural change concerning financial conduct when supported by structured models of delivery (Srivastava et al., 2019). However, issues, such as dormant accounts, infrastructural bottlenecks, and the absence of any form of regularly maintained awareness programs, still prevail (Gupta, 2023; Somani and Nahar, 2015).

Objectives

- Assess the extent of digital risks faced by PMJDY beneficiaries, especially in rural and semi-urban areas.
- Evaluate the effectiveness of existing legal and institutional frameworks, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023.
- Investigate real-world cases of cyber fraud and privacy violations linked to PMJDY transactions.

Research Gap

While PMJDY has been widely studied from the lens of financial inclusion, the cybersecurity and data privacy dimensions of its digital implementation remain relatively underexplored. Existing literature focuses predominantly on access and account penetration, with limited scholarly attention to the risks borne by digitally inexperienced users. There is a notable gap in empirical and policy analysis on how cyber threats such as phishing, SIM swaps, and biometric misuse specifically affect PMJDY users. Furthermore, while new legislation like the DPDP Act, 2023, signals progress, its implementation challenges, particularly for marginalized populations, remain unaddressed in current academic discourse.

Research Methodology

This research paper observes a qualitative as well as analytical research approach in investigating issues or challenges regarding cybersecurity and data privacy risks involved with the digital transaction of PMJDY. The secondary data was widely collected through the works of scholars,

government publications, legal frameworks, and empirical studies on topics of financial inclusion, cybersecurity, and digital infrastructure in India. The theoretical learning was tested concerning real-life cases of fraud that involved PMJDY users to see how the theoretical application would work in the real world and reveal any system failures. The paper also considers findings of official financial inclusion statistics during 2018-2024, including growth of accounts, digital fraud cases, and dormant account levels. Special attention was paid to examine the effectiveness of legal policy instruments like the Information Technology Act, 2000, and the Digital Personal Data Protection (DPDP) Act, 2023. Content analysis was used to identify the recurrences in the themes connected to Aadhaar-based identity misuse, SIM swapping, phishing, and insider threats. Digital literacy gap and institutional gaps were also analyzed under the descriptive statistics and risk matrix analyses, and tested to determine the extent of threat and the causes of threats of digital threats. The methodology will give an all-around appreciation of the ecosystem strengths and weaknesses, particularly through the eyes of vulnerable classes. This interpretive method can be utilized efficiently, further setting up guidelines aimed at improving and advancing digital security and privacy in the PMJDY on the currently manifesting platform.

Findings

The study finds that the rapid digital adoption under PMJDY has inadvertently created a vulnerable ecosystem, especially for first-time users. Phishing, malware, OTP theft, and SIM swapping are among the most prevalent threats. Many users operate on low-cost smartphones without proper security protections, and awareness of safe digital practices is alarmingly low. Aadhaar-based authentication, while streamlining transactions, has raised serious concerns around biometric data misuse. Additionally, data sharing through intermediaries occurs with little to no user consent, and redressal mechanisms are either weak or inaccessible. Institutional adherence to security protocols is inconsistent, and insider threats—from banking correspondents or fintech providers—further compromise user safety.

Analysis

Pradhan Mantri Jan Dhan Yojana (PMJDY) is an entire financial authorizing agenda to individuals (Indians) who have been barred from formalized financial frameworks of millions in India. It hopes to give access to banking and financial services to everyone in such a way that even the marginal communities can enjoy the booming Indian economy. The major goal of PMJDY is the provision of access to banking services to all citizens, because a large part of the population of India, especially in remote and rural territories, was not within the framework of the formal banking system at all. In helping citizens open bank accounts with zero balances in banks, the PMJDY scheme has greatly lowered the threshold to entry by millions who could not access bank services either on physical, economic, or educational grounds. Banks have been able to extend their services to rural areas and under-represented communities and mostly with the support of the business correspondents, and move banking to the doorstep of the people.[5]

The government is putting much emphasis on financial literacy to enhance effective financial inclusion, at least among the rural beneficiaries. The work on such themes as saving, credit management, digital payments, and fraud awareness is underway. These initiatives enable the users to make their choices consciously and decrease their exposure to schemes. The government agencies, banks, and NGOs carry out awareness camps and training in the local language, closing the digital and knowledge gap.[6]

With the help of PMJDY, Direct Benefit Transfers (DBTs) will be provided promptly without the involvement of intermediaries and with minimal leaks. It is integrated with Aadhaar to enable quicker and safer transfer. Micro-credit and insurance products also gain access to poor people through the PMJDY. The plan provides economic insurance cover and risk covers, which would lead to financial security and resilience of the vulnerable family members.[7]

Digital Components

The success and expansion of PMJDY are intrinsically linked to its integration with India's evolving digital financial ecosystem. Digital platforms have been leveraged to deliver banking and payment services efficiently and at scale, reaching even the remotest corners of the country.

A key digital enabler is the **Aadhaar-enabled Payment System (AePS)**. AePS provides its customers of the bank with the capability to conduct low-value banking activities based on their Aadhaar number and through biometric verification rather than through debit cards or PINs. This system has especially had a significant effect in rural settlements where large numbers of users might not possess or might not understand the process of using physical cards; they can, however, verify themselves biometrically. AePS enables business correspondents to conduct cash withdrawals, check balances, and send money via micro-ATMs. This biometric authentication process is an industry game changer, as people with limited literacy levels can have convenient access to bank facilities and have a secure and paperless way of doing it.[8]

Complementing AePS is the **Unified Payments Interface (UPI)**, which has transformed digital payments across India. UPI is a mobile program where instant transfer of money can be made between bank accounts without revealing any critical information. The ease of use, low transaction cost, and interoperability have attracted the beneficiaries of PMJDY to use the service. UPI saves the use of cash and gives ease of use to those who cannot have a formal financial interaction, and thus, it will be a potent instrument for paying and receiving cash.

Mobile banking and SMS alerts are other critical components of the digital ecosystem supporting PMJDY. Mobile bank applications allow checking balances, sending money, and using other banking services. SMS alert is a must, especially for customers with less knowledge in operating a smartphone, and it offers real-time performance concerning the transactions. This is since an instant feedback loop builds confidence in the banking system as well as enables the user to keep track of their finances in a real-time manner, increasing their access to banking services.[9]

Lastly, the introduction of **RuPay debit cards** under PMJDY has expanded financial access and convenience. RuPay is an indigenous debit card payment system in India, and it is made to provide low-cost and cheap debit card services. The cardholders are able to deposit and cash out the cards in the ATMs, point of sale terminals, and go online using these types of cards. The high adoption of RuPay cards in the Indian banking system guarantees the fact that the target population of PMJDY will be able to join the formal financial system in a safe and effective way. Furthermore, RuPay cards usually have options that cater to the low-income client through lower or no annual fees, promoting the aspect of financial inclusion.[10]

Data Privacy Concerns in PMJDY Digital Transactions

- **Exposure through Unregulated Data Access and Sharing**

The rural and underserved areas where PMJDY account owners live frequently have to resort to middlemen such as local agents or banking correspondents to use digital financial services. This model has brought about accessibility, but has brought about risks due to the fact that people are always talked into giving out confidential information without having the slightest idea of how they will use it or how it will be stored. The informally performed actions, interactions with little protection, provide an ability to collect and share data without the understanding and control of the data user. This has prompted cases of data misuse in terms of accessing funds, committing a fraudulent transaction, or enrollment in financial instruments without consent. The absence of a unified solution to the problem of data treatment also adds another problem to the stack, as the users are always under the threat of identity theft and financial fraud.[11]

- **Lack of Awareness Regarding Data Protection Rights**

India's **Digital Personal Data Protection Act (DPDP), 2023,** is a significant step toward strengthening privacy protections for citizens. It specifies rights like the right to give informed consent, and see personal data, as well as withdraw consent. Nevertheless, most of the beneficiaries of PMJDY cannot avail of these legal rights, namely, low-literate ones or those lowly exposed to technology. The majority of users do not know that they even have the right to inquire about the use of their data. The consent forms, when used, are usually elaborate, vaguely explained, or in a language that the user does not understand. Consequently, there is a lot of passive consent wherein users have no real idea of what they agreed to accept. There may be a temptation to divulge personal information only in order to make a transaction, and be unaware of the future consequences.[12]

- **Risks from Poor Data Storage and Retention Practices**

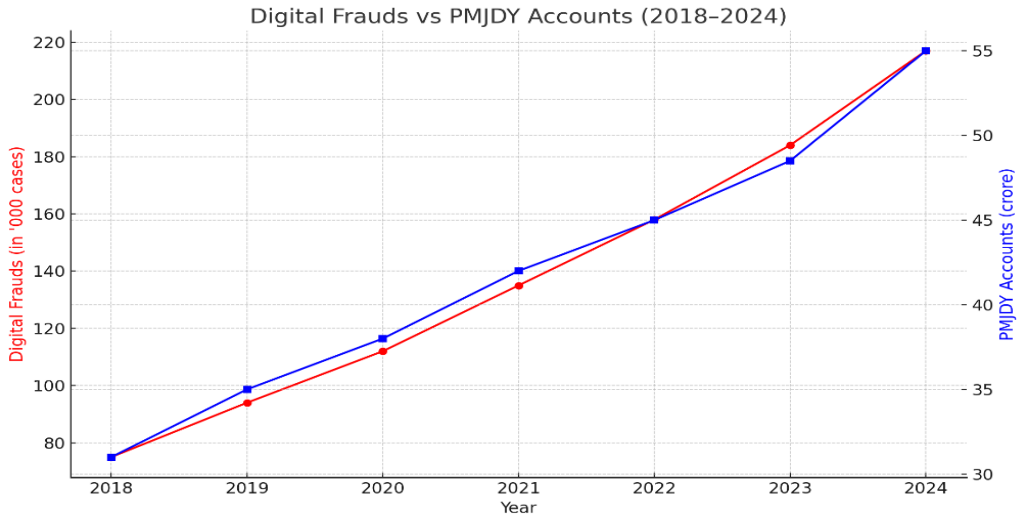
Besides the collection of the data, its storage is also another questionable aspect, where there is a period during which it should last. Due to the way it is framed, banks and digital service providers working by the PMJDY paradigm collect enormous user data aimed at accessing biometrics, identity documents, and transaction history. Nevertheless, there is no standard that you should follow for the length of retention and the way this data should be retained. In other instances, the information of the user is retained indefinitely even after it has outlived its usefulness. This creates a pool of old but sensitive data that the cybercriminals could target. The cybersecurity protocols of smaller service providers, especially, may be weak. Their systems might be unencrypted, security audits not performed properly, and their servers not being secure in order to avoid leak of data leaks and hacking.[13]

Data Analysis of PMJDY's Digital Risks and Infrastructure

A critical examination of the data underpinning PMJDY's digital infrastructure reveals a dual-edged outcome: one of growth and outreach, and another of exposure and fragility. From 2018 to 2024, the number of PMJDY accounts increased from 31 crore to 55 crore. On the surface, this trajectory signals successful mass inclusion. However, this quantitative expansion coincided with a troubling rise in digital fraud cases—from 75,000 in 2018 to 217,000 by 2024—illustrating a growing attack surface within India's financial ecosystem.

Table 1: Growth in PMJDY Accounts and Digital Fraud Cases (2018–2024)

Year	PMJDY Accounts (crore)	Digital Frauds ('000 cases)	Dormant Account %
2018	31.0	75	41%
2019	35.0	94	38%
2020	38.0	112	35%
2021	42.0	135	30%
2022	45.0	158	26%
2023	48.5	184	21%
2024	55.0	217	18%



While the percentage of dormant accounts has gradually decreased from 41% to 18%, the figures remain high. Nearly one in five accounts remains inactive, highlighting partial and passive usage. The dormant accounts tend to be more vulnerable to silent exploitation, particularly when it comes to the Aadhaar-based form of biometric misuse, where not every user might keep track of their transaction history regularly. The digital fraud that has rocketed could be blamed on various infrastructural shortcomings. A good number of users of PMJDY use a shared device, a low-end smartphone, and unsecured networks under which the systems can be prone to malware, phishing, and SIM swap. Such types of fraud are usually based on the lack of robust endpoint protection and the digital illiteracy of the user. To use a more specific example, although UPI and AePS systems are fast and convenient, their performance regarding security is limited to the knowledge of a user and the encryption protocol, which is maintained by the backend.

Table 2: Key Risks in PMJDY Digital Ecosystem

Risk Factor	Severity	Underlying Cause
SIM Swapping & OTP Theft	High	Poor telecom security, low awareness
Aadhaar-based Identity Misuse	High	Centralized biometric storage, lack of MFA
Fake Apps and Phishing	Medium	Digital illiteracy, unverified app markets
Dormant Account Exploitation	Medium	Passive users, unmonitored balances
Insider Data Misuse (e.g., by BCs)	Medium	Weak institutional oversight

The reliance on biometric authentication without robust fallback mechanisms further adds to system fragility. Unlike passwords, biometric data cannot be reset once compromised, exposing users to lifelong risk if their identity is cloned or leaked. Additionally, legal frameworks like the **DPDP Act, 2023**, though progressive, lack operational traction in rural India, where awareness of consent rights and redressal processes is minimal.

Result and Discussion

In line with the findings of this research study, a critical paradox with the Pradhan Mantri Jan Dhan Yojana (PMJDY) scheme has been that as the scheme has been very effective in increasing financial inclusion by adding nearly 55 crores of the population to the formal banking system by 2024, it has also contributed to exposing a high proportion of its user base to serious cyber threats and data privacy risks. A gap between technology access and digital security is illustrated as the number of digital frauds increases exponentially with the growth of accounts in the PMJDY service, as the number of digital frauds in 2018 was 75,000, and by 2024 expected to exceed 217,000. The simultaneous decline in account dormancy, which reduced the rate to only 18 percent, can be discussed as a positive indicator of usage, but is not enough to ensure the financial safety of accounts, which still can be exposed to being penetrated authentically in dormant accounts and those checked occasionally only (especially in the case of Aadhaar-linked systems with no multi-factor authentication and its use).

The argument sheds light on the convoluted interaction of technology infrastructure, socio-economic weaknesses, and policy gaps, which characterize the digital ecosystem of PMJDY. Whereas financial transactions in Aadhaar-enabled Payment Systems (AePS), UPI, mobile banking systems, among others, have been democratized, their adoption in systems where there is a lack of digital literacy, security of devices, and awareness among users has contributed to incomplete, even detrimental integration of these mechanisms. In the case of most PMJDY account users, especially in rural locations, there is a lack of support systems that come with switching to digital banking, including safe devices, encrypted connections, and cyber hygiene education. Because of this, users are exposed to the hazards of phishing, SIM swaps, and malware without knowing they are the targets, and they are unable to not only know of the risks but also have a way of seeking redress.

Recommendations

In order to improve the security and privacy of the digital transactions in the Pradhan Mantri Jan Dhan Yojana (PMJDY), the immediate and long-term need must be large-scale and long-term digital literacy. The foremost causes of most cyber frauds among PMJDY account holders are preliminary digital illiteracy, which can be explained in the following way: choosing the right links, working safely with OTPs, and not responding to calls or applications that might just be an attempt to get your money. The government, through its partnership with banks, NGOs, and local institutions, must carry out frequent and multilingual awareness initiatives with easily comprehensible and relatable content. Particular emphasis should be placed on rural regions that have little technological exposure. Cyber hygiene, safe mobile, and grievance redressal module should be embedded in the training plan, and the beneficiaries should be prepared to identify and deal with threats.

Second, technological protection should be greatly enhanced. Though the authentication based on Aadhaar makes it fail-safe to access, the excessive use of the same without multi-factor authentication (MFA) is risky. Banks and makers of digital services ought to use MFA as often as they can, using either biometric or OTP identification coupled with PINs or application-based approvals. Additionally, transaction electronics and applications should be encrypted following robust protocols and will be periodically checked in terms of security. It should also enable the service providers to take the blame due to any failure in cybersecurity infrastructure in case such failures compromise the data of the users or cause financial fraud.

Third, legal frameworks and regulations, in particular, the Digital Personal Data Protection (DPDP) Act, 2023, should be enforced with much more outreach and transparency. Currently, the majority of users do not realize their data rights, and in many cases, the process of consent is not transparent or even unintelligible. Understandably, location-specific consent forms and disclosures need to be made compulsory, and a user needs to have easy means to access the opportunity to view, change, or put an end to the consent of their data sharing. Also, a user-friendly, centralized grievance redressal system must be formulated where the victims of any digital fraudulence or misuse of data can seek redressal on an urgent basis, which may include any legal support in cases of prompt need. Regulatory agencies should also step up surveillance of business correspondents and intermediaries to arrest the tendency of insider abuse and unauthenticated data manipulation.

Finally, a coherent, proactive security approach should be put in place in the digital financial ecosystem that supports the PMJDY. This should comprise a real-time fraud monitoring and detection system, a national incident response team in the case of breaches related to Aadhaar links, and regular risk assessment of providers of financial services. The government incentives or subsidies can help attract the solutions of the private companies to increase the security levels in the apps focusing on the PMJDY users. The Ministry of Electronics and Information Technology (MeitY), UIDAI, RBI, and banks should collaborate in achieving sustainable interaction of privacy and cybersecurity requirements. A multi-stakeholder approach is the only way of ensuring that the digital transformation of PMJDY is achieved for the most vulnerable recipients.

Conclusion

The Pradhan Mantri Jan Dhan Yojana (PMJDY) has been one of the most significant steps toward financial inclusion in India’s history. By opening the doors of formal banking to millions, particularly in rural and underserved areas, the initiative has transformed how people save, spend, and receive benefits from government welfare schemes. However, the rapid integration of digital platforms into this ecosystem has brought with it an equally urgent need to address cybersecurity vulnerabilities and data privacy concerns, especially for those who are new to the digital world.

This research has highlighted that while PMJDY has successfully enabled digital financial participation, it has also unintentionally exposed its beneficiaries to risks they are often unprepared to deal with. A lack of digital literacy, inadequate legal enforcement, and gaps in institutional security measures all contribute to a fragile ecosystem. In many cases, users unknowingly share sensitive information, fall prey to fraud, or are left helpless when breaches

occur. These are not just technical problems—they have real, human consequences, especially for those already on the margins of society.

The current legal and regulatory framework, though significant in its intent, still lacks the agility to keep up with fast-evolving cyber threats. While laws like the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, offer a foundation for user protection, they require more effective implementation, especially when it comes to PMJDY beneficiaries. Legal provisions must not only exist—they must be understandable, accessible, and enforceable at the grassroots level.

Moreover, cybersecurity is not only a legal or technological issue; it is also deeply social. Empowering people with the knowledge to protect their data and understand their digital rights is just as crucial as implementing encryption and secure networks. In this regard, community-driven awareness campaigns, local-language education materials, and inclusive outreach models can make a tremendous difference. When users understand the value of their data and how to protect it, they become active participants in their security.

Strategic interventions such as improved digital education, stronger institutional safeguards, user-friendly consent processes, and a centralized incident response mechanism are necessary next steps. These interventions must be designed with empathy and practicality, recognizing the diverse needs, capacities, and limitations of PMJDY users. Technology should not widen the gap between the informed and the unaware; instead, it should act as a bridge to inclusion, safety, and dignity.

REFERENCES

Bhisham Kapoor & Ekta Tyagi, Role of Pradhan Mantri Jan Dhan Yojana in Digital Financial Inclusion, 29 INT'L J. Advanced Sci. & Tech. (2020) – 238

Sudhanshu Sekhar Tripathy, A Comprehensive Survey of Cybercrimes in India Over the Last Decade, (Apr. 21, 2025), https://arxiv.org/abs/2505.23770 - 1

Muneeb Ul Hassan, Mubashir Husain Rehmani & Jinjun Chen, Differential Privacy in Blockchain Technology: A Futuristic Approach, arXiv (Oct. 10, 2019), https://arxiv.org/abs/1910.04316 - 1

Noe Elisa et al., A Framework of Blockchain-Based Secure and Privacy-Preserving E-Government System, arXiv (June 25, 2020), https://arxiv.org/abs/2006.14231 - 1

AKM Bahalul Haque & Mahbubur Rahman, Blockchain Technology: Methodology, Application and Security Issues, arXiv (Dec. 24, 2020), https://arxiv.org/abs/2012.13366 - 1

A.K. Srivastava, K.C. Sharma & D.V. Deshpande, Policy Induced Financial Inclusion: A Case of Pradhan Mantri Jan Dhan Yojana (PMJDY) in Uttar Pradesh, 38 J. RURAL DEV. 322 (2019), https://doi.org/10.25175/jrd/2019/v38/i2/146748 - 322

Ravikumar T, Pradhan Mantri Jan-Dhan Yojana: An Evaluation, 17 USHUS J. BUS. MGMT. 9 (2018), https://doi.org/10.12725/ujbm.44.2 - 9

Ramasethu, Pradhan Mantri Jan Dhan Yojana: The Most Intensive Financial Inclusion Scheme in India, 2 INT L EDUC. & RES. J. (2016), https://ierj.in/journal/index.php/ierj/article/view/297 - 1

Reshma Kurussiveettil & K. Kanniammal, Impact of Literacy on Pradhan Mantri Jan Dhan Yojna Awareness and Financial Inclusion: Evidence from Scheduled Tribes of Kerala, 22 S. INDIA J. SOC. SCI. (2024).

M.D. Somani & Bhavana Nahar, Pradhan Mantri Jan Dhan Yojana: Financial Inclusion, 10 J. COM. & TRADE (2015) – 1

Kamakshi Malik, The Impact of Pradhan Mantri Jan-Dhan Yojana on Financial Inclusion in India, 2 INT L J. BUS. & MGMT. (2014), https://www.internationaljournalcorner.com/index.php/theijbm/article/view/138064 - 31

S.S. Chowhan & J.C. Pande, Pradhan Mantri Jan Dhan Yojana: A Giant Leap Towards Financial Inclusion, 1 INT L J. RES. MGMT. & BUS. STUD. 19 (2014) – 19

K. Vinit, Pradhan Mantri Jan Dhan Yojana (PMJDY): Financial Inclusion and Inclusive Growth in India, 3 INT L J. SCI. & INNOVATIVE RES. STUD. (2015) - 1