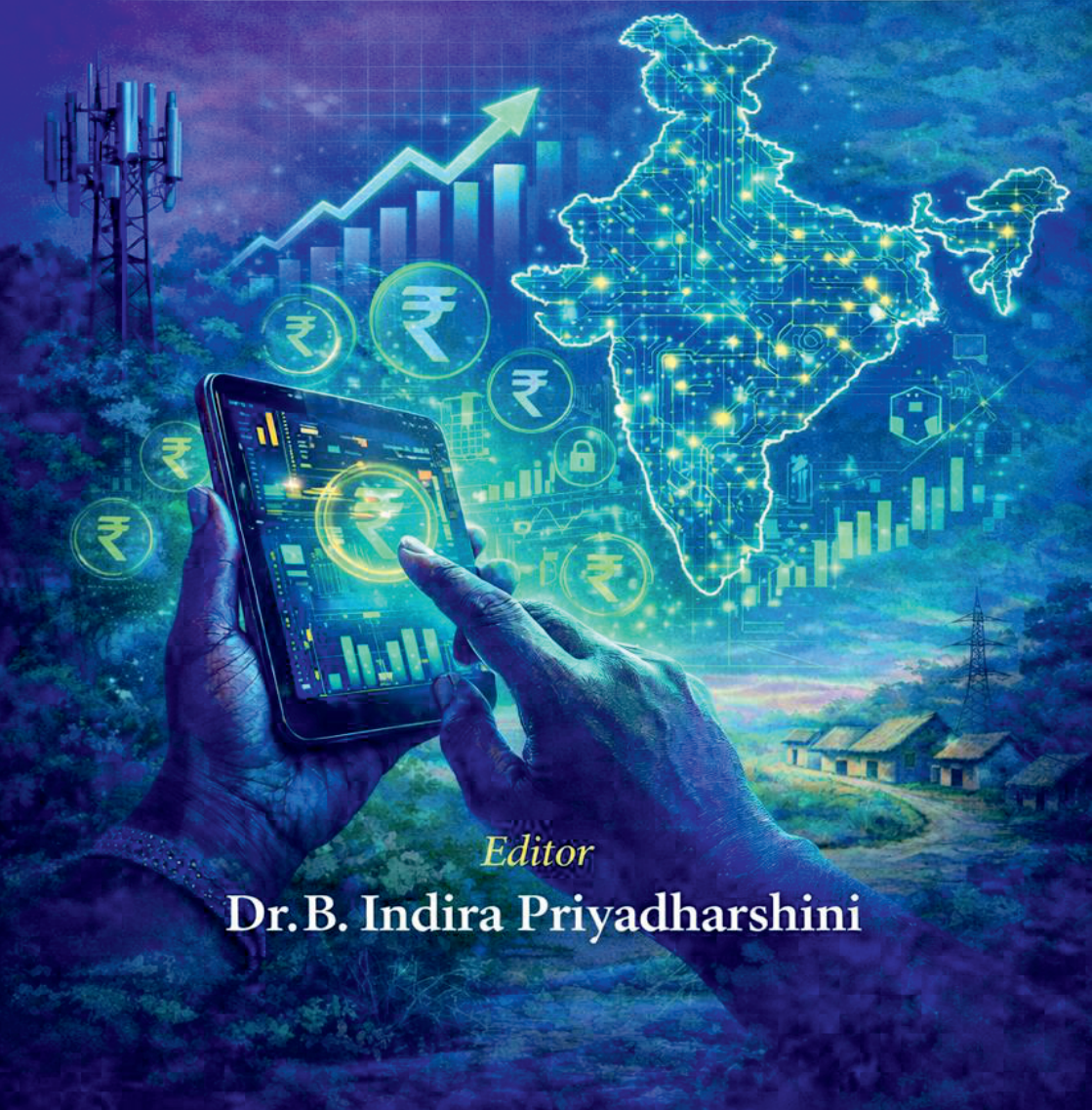


Empowering the Marginalized

Digital Finance as a Tool for Social Inclusion



Editor

Dr. B. Indira Priyadharshini

EMPOWERING THE MARGINALIZED : DIGITAL FINANCE AS A TOOL FOR SOCIAL INCLUSION

Editor

Dr. B. Indira Priyadharshini

Empowering the Marginalized : Digital Finance as a Tool for Social Inclusion

Dr. B. Indira Priyadharshini

Assistant Professor

Department of Commerce (CA), NGM College, Pollachi

First Edition : January 2026

ISBN : 978-93-5602-712-1

Price : Rs. 850/-

Copyright All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the author.

Printed at

CAUVERITECH Computerised Print Shop

21/2, Rajamill Road, Pollachi – 642 001.

Ph : 04259 – 221734

E-Mail : cauveritech@gmail.com

45.	GOVERNANCE OF DIGITAL PUBLIC INFRASTRUCTURE IN INDIA : THE CASE OF INDIA STACK <i>Mr. M. Prem & Mr. G. Jeevanantham</i>	311
46.	ROLE OF PUBLIC SECTOR BANKS AND REGIONAL RURAL BANKS IN DIGITAL TRANSFORMATION <i>Ms. M. Satheeswari, Ms. M. Haripriya & Dr. R. Manikandan</i>	315
47.	CHALLENGES IN DATA PRIVACY, SECURITY AND KYC FOR THE MARGINALIZED <i>Mrs. M. Ragaprabha & Ms. K. Karthika</i>	328
48.	ROLE OF ADDRESSING THE GENDER GAP IN DIGITAL FINANCE <i>Mrs. M. Ragaprabha & Mr. G. Arish</i>	336
49.	SUSTAINABLE AND GREEN FINANCE THROUGH DIGITAL CHANNELS <i>Dr. A. Albina, Ms. T. Kavipriya & Ms. J. Abinaya</i>	343
50.	SOCIO-ECONOMIC DETERMINANTS OF DIGITAL EXCLUSION : AN ANALYTICAL STUDY <i>Mr. M. Prem & Ms. K. Vanita</i>	353
51.	CHALLENGE IN LAST-MILE : CONNECTIVITY AND HARDWARE <i>Mrs. M. Ragaprabha & Mr. V. Mohan Raj</i>	358
52.	BRIDGING THE GAP : TRANSFORMING FINANCIAL EXCLUSION INTO DIGITAL INCLUSION THROUGH PRADHAN MANTRI JAN SURAKSHA SCHEMES <i>Dr. S. Kaleeswari</i>	364
53.	FINTECH INNOVATIONS IN RURAL INDIA AND THEIR SOCIAL IMPACT <i>Mrs. C. Akila, Ms. K.G. Manasvini & Ms. S. Revathi</i>	371

CHALLENGES IN DATA PRIVACY, SECURITY AND KYC FOR THE MARGINALIZED

Mrs. M. RAGAPRABHA, Assistant Professor,
PG Department of Commerce with International Business, NGM College, Pollachi.

Ms. K. KARTHIKA, I M.COM IB,
NGM College, Pollachi.

ABSTRACT

The rapid expansion of digital services has increased the importance of data privacy, security, and Know Your Customer (KYC) frameworks in financial and governance systems. However, marginalized populations including low-income groups, rural communities, migrants, women, and informal workers often face significant challenges in accessing these systems due to limited digital literacy, lack of formal identification, and inadequate infrastructure. This paper examines the intersection of data privacy, security, and KYC processes in the context of marginalized communities, highlighting how exclusionary design and weak data protection mechanisms can deepen social and economic inequalities. It explores key risks such as data misuse, surveillance, identity theft, and consent violations, which disproportionately affect vulnerable groups. The study also examines existing regulatory frameworks and digital identity initiatives, with a focus on balancing financial inclusion and individual rights. The paper concludes by emphasizing the need for inclusive KYC models, robust data protection laws, and community-centric digital literacy programs to ensure secure, equitable, and rights-based access to digital services for marginalized populations.

Key Words : Challenges, Data Privacy, Security, KYC.

INTRODUCTION:

Digital systems today play a major role in delivering financial, welfare and communication services. However, marginalized groups such as rural communities, migrants, low-income households and the elderly often face barriers in accessing these systems. Ensuring strong data privacy, robust data security and inclusive KYC processes is essential for protecting their rights and enabling equal participation in the digital economy. These regulations are essential for safeguarding the financial system. However, they also introduce significant data privacy concerns, raising questions about how companies can protect sensitive customer information without

compromising compliance. Balancing Know Your Customer requirements with data privacy is critical for businesses operating in today's regulatory environment. Implementing best practices can help organizations ensure compliance while safeguarding sensitive customer information.

OBJECTIVES :

- To analyze the challenges faced by marginalized communities in accessing digital services due to KYC and data privacy frameworks.
- To identify key risks related to data misuse, surveillance, and consent violations.

KEY ISSUES AND CHALLENGES:

1. Exclusion Due to Rigid KYC Norms:

One of the most significant challenges in digital service delivery is the rigid and documentation-heavy nature of KYC requirements. Marginalized communities such as migrants, daily wage workers, rural populations, and women without independent identity documents often lack essential proofs like Aadhaar, PAN, birth certificates, or valid address records. Many individuals also face difficulties with biometric authentication due to age, manual labour, or malfunctioning devices. As a result, they are frequently denied access to bank accounts, SIM cards, welfare schemes, insurance, pensions, and digital payment systems. The dependence on formal identification systems, without considering socio-economic realities, creates structural barriers that deepen financial and social exclusion.

2. Limited Digital Literacy and Technological Skills:

A major obstacle for marginalized populations is their limited exposure to digital technologies. Many individuals struggle to understand online processes, operate smart phones, navigate apps, or identify fraudulent links. Because of this lack of digital confidence, they often depend on intermediaries such as shopkeepers, agents, or cybercafé operators to complete transactions. This dependence increases their risk of exploitation, overcharging, data theft, and unauthorized access to personal accounts. Furthermore, digital interfaces are often designed in English or complex language, making them inaccessible for individuals with low literacy levels. Thus, limited digital skills not only restrict participation but also heighten vulnerability to fraud and misinformation.

3. Data Privacy and Security Risks:

Marginalized groups face heightened risks of data misuse due to weak privacy protections, inadequate awareness, and excessive data collection. When individuals share biometric data, mobile numbers, or documents without fully understanding the consequences, they become susceptible to identity theft, fraud, unauthorized data sharing, and profiling. In many cases, users provide consent automatically without informed understanding, leading to consent violations. Additionally, centralized digital identity systems create opportunities for surveillance, where movement, transactions, and personal information may be monitored or misused. The lack of strong encryption practices, poor cyber security infrastructure, and frequent data breaches further increase the vulnerability of these populations.

4. Inadequate Digital Infrastructure:

Insufficient digital infrastructure remains a major barrier, especially in rural and remote regions. Many areas still lack stable internet connectivity, affordable data plans, or uninterrupted electricity, making digital verification processes unreliable. Shared mobile phones are common in low-income households, increasing the risk of unauthorized access, loss of privacy, and data exposure. Poor-quality devices and outdated software also prevent secure authentication and limit the ability to use advanced digital services. Without strong infrastructure, even well-designed digital systems fail to reach or benefit marginalized communities.

5. Language Barriers and Accessibility Issues:

Digital services are often developed without considering linguistic diversity or accessibility needs. Many platforms provide instructions only in English or in complex technical language that is difficult for first-time users. For people with disabilities such as visual impairments, hearing limitations, or motor challenges digital systems often lack supportive features like screen readers, voice navigation, or simplified interfaces. These design limitations create additional layers of exclusion for vulnerable groups who already face economic and social disadvantages.

6. Dependence on Biometric Authentication:

Biometric-based KYC systems, while convenient, pose several challenges. Individuals with worn-out fingerprints (common among manual labourers),

elderly persons, or those with disabilities often face repeated authentication failures. Environmental factors, such as humidity or dust, can also affect biometric accuracy in rural areas. When biometric verification fails, individuals may be denied essential services, including subsidy withdrawals or welfare payments. Moreover, the storage of biometric data increases privacy risks if not protected with strong safeguards.

7. Trust Deficit and Fear of Surveillance:

A lack of trust in digital systems is widespread among marginalized communities. Many individuals fear that their personal information may be misused by authorities, employers, or private actors. Past incidents of data leaks, phishing scams, and financial fraud have increased scepticism toward digital systems. This lack of trust discourages people from adopting digital services even when they could benefit from them. Fear of surveillance especially among migrant workers or informal workers further limits their willingness to share data.

8. Gender-Based Barriers:

Women in marginalized groups face unique challenges, such as limited phone ownership, restricted mobility, lower literacy rates, and cultural norms that limit decision-making. Many women rely on family members to access digital services, which reduces their privacy and autonomy. Safety concerns, online harassment, and lack of digital awareness further discourage women from using digital platforms independently. These gender-specific challenges contribute to a widening digital gender gap.

9. Weak Grievance Redressal Mechanisms:

Many users lack access to effective support systems to resolve issues such as failed authentication, incorrect data, fraud, or system errors. Customer service centres are often far away, unresponsive, or linguistically inaccessible. As a result, marginalized individuals face delays, financial loss, or incorrect data records without any reliable way to correct them. This weakens their trust in digital systems and makes them hesitant to engage with digital platforms again.

RISKS IN DATA MISUSE, SURVEILLANCE, AND CONSENT VIOLATIONS:

1. Data Misuse and Unauthorized Sharing:

One of the fundamental risks associated with digital identity systems is the misuse of personal data. Marginalized individuals often share sensitive information such as Aadhaar numbers, biometric details, bank account information, and phone numbers without fully understanding where this data will be stored or how it will be used. Due to weak monitoring and limited accountability, this data may be accessed by unauthorized third parties, sold to private companies for profit, or used for targeted advertisements. In many cases, intermediaries handling digital transactions misuse or copy people's documents without their knowledge. Such unauthorized sharing can lead to financial fraud, identity duplication, and long-term vulnerabilities for individuals who lack the resources to protect themselves or seek legal recourse.

2. Identity Theft and Financial Fraud:

Identity theft is a major threat for digitally inexperienced users. When personal information is leaked or mishandled, fraudsters can impersonate individuals to open bank accounts, take loans, conduct unauthorized transactions, or access government welfare schemes. Biometric data, once compromised, cannot be replaced like a password. Marginalized populations are especially vulnerable because they may not regularly monitor their bank accounts, possess cybersecurity awareness, or have access to quick grievance redressal mechanisms. This increases the chances of prolonged financial loss, exploitation, and emotional distress.

3. Surveillance and Tracking Risks:

Digital identity systems and centralized databases enable the possibility of continuous monitoring of individuals' activities. Governments and private companies can track people's movements, financial transactions, mobile usage, and behavioral patterns, often without explicit consent or awareness. For marginalized communities such as migrants, informal workers, or minority groups this creates a climate of fear and distrust. Surveillance can also be used to restrict mobility, target specific populations, or monitor social and political activities. Over time, such practices may lead to loss of

autonomy, reduced participation in digital services, and deeper social marginalization.

4. Profiling and Algorithmic Bias:

When large volumes of personal data are collected, individuals risk being profiled based on their demographic, socio-economic, or behavioural characteristics. Automated systems may categorize users as “high-risk” or “low-risk,” influencing their access to loans, welfare benefits, or employment opportunities. Algorithmic bias where digital systems unintentionally discriminate against certain groups can further reinforce inequalities. For example, low-income or rural individuals may be algorithmically flagged as unreliable borrowers due to their transaction patterns, preventing them from accessing financial services. Such profiling, when done without transparency or accountability, can deepen existing discrimination.

5. Consent Violations and Lack of Informed Choice:

Most digital platforms require users to provide consent before collecting or processing data. However, marginalized populations often cannot read or understand consent forms, which are typically written in complex legal language or non-local languages. As a result, they provide consent without realizing what data is collected, how it will be used, or with whom it may be shared. This is known as “blind consent” or “forced consent.” In many cases, digital services are designed in a way that denies access if the user refuses to share their data, leaving them no meaningful choice. These violations undermine the principle of informed consent and expose vulnerable individuals to long-term privacy risks

6. Weak Security Protections and Frequent Data Breaches:

Many digital systems, especially in developing countries, lack strong cyber security measures such as encryption, secure authentication, or regular audits. As a result, government databases, banking systems, and private platforms are prone to hacking and data breaches. When a breach occurs, sensitive information including biometrics, identities, financial details, and health records is exposed to cybercriminals. Marginalized individuals rarely receive notifications about such breaches, nor do they have the tools to protect themselves afterward. This increases the risks of lifetime exploitation, as stolen identity data cannot be easily changed.

7. Misuse by Intermediaries and Local Operators:

In rural areas or low-income settings, users often depend on agents, cybercafé operators, or mobile shop owners to complete digital transactions. These intermediaries sometimes misuse documents by storing photocopies, accessing OTPs, or linking their own numbers to user accounts. Such practices make marginalized users vulnerable to fraud, unauthorized transactions, and breach of privacy. The absence of regulatory oversight and lack of digital awareness among users allow such exploitation to go unnoticed.

8. Long-term Data Exploitation and Loss of Autonomy:

Once personal data is collected, it often stays in digital databases indefinitely. Marginalized individuals have minimal control over how long their data is stored, how it is processed, or whether it can be deleted. This loss of autonomy can have long-term consequences, including exclusion from services, manipulation, targeted misinformation campaigns, and discrimination. The inability to control personal data erodes trust in digital systems and prevents meaningful digital participation.

CONCLUSION:

For marginalized communities, data privacy, security, and inclusive KYC processes are crucial to ensure equal access, protection of rights, and participation in the digital economy. Governments and institutions must implement safe, fair, and accessible systems that empower the vulnerable rather than exclude them. An era of rapid digital transformation, ensuring data privacy, security, and inclusive KYC practices is not only a technical requirement but a social responsibility. Marginalized communities remain the most vulnerable to digital risks, including data misuse, identity theft, and systemic exclusion due to documentation gaps or technological barriers. Strengthening legal safeguards, improving cybersecurity infrastructure, and promoting transparent data governance are essential to protect their rights. At the same time, simplifying KYC procedures, offering alternative identity options, and providing assisted digital services can significantly reduce exclusion. Ultimately, building a fair digital ecosystem requires balancing innovation with inclusion, ensuring that technological progress uplifts every individual.

REFERENCE:

1. OECD (2020). Digital Transformation and the Vulnerable Communities. Focuses on digital risks and protections for excluded populations
2. UNCTAD (2021). Data Protection and Privacy Legislation Worldwide. Examines global privacy issues and digital inclusion.
3. Sarkar, S. (2021). “Digital Exclusion and Data Rights in India.” Economic and Political Weekly. Discusses how marginalized communities face exclusion in digital systems.
4. Study on demographic privacy in South Africa (2022) – explores varied privacy concerns across demographic groups, useful for comparative context.
5. et al. (2025) – Minorities ethnic people’s security and privacy concerns with essential online services — qualitative interview study showing how privacy concerns impact marginalized groups’ online engagement.
6. et al. (2025) – Secure Sharing of Identity (KYC) — block chain-based model for secure, privacy-preserving KYC data sharing (important for constructing inclusive digital identity systems).
