



# FinTech *for the* Last Mile

---

Financial Inclusion in the Era of Amrit Kaal

---

Dr. B. Indira Priyadharshini

Mr. A. Prakalathan

Dr. D. Saranya

Dr. M. Nirmala

## **FinTech for the Last Mile : Financial Inclusion in the Era of Amrit Kaal**

**Dr. B. Indira Priyadharshini**

*Assistant Professor*

*Department of Commerce (CA), NGM College, Pollachi*

**Mr. A. Prakalathan**

*Assistant Professor*

*Department of Commerce (CA), NGM College, Pollachi*

**Dr. D. Saranya**

*Assistant Professor*

*Department of Commerce (CA), NGM College, Pollachi*

**Dr. M. Nirmala**

*Assistant Professor*

*Department of Commerce (CA), NGM College, Pollachi*

**First Edition : January 2026**

**ISBN : 978-93-94004-59-7**

**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](mailto:cauveritech@gmail.com)

## **PROTECTING DATA RIGHTS OF MARGINALIZED GROUPS :\_PRIVACY, SECURITY & KYC**

**Dr. G. VIGNESH**

Associate Professor & Head – PG Department of Commerce IB, NGM College

**Ms. S. JEEVITHA**

Student, PG Department of Commerce IB, NGM College

### **ABSTRACT**

*Marginalized communities often face significant barriers in accessing financial, digital, and governmental services due to strict Know Your Customer (KYC) norms, poor digital literacy, and inadequate data protection. This paper examines the intersection of data privacy, security, and KYC requirements, highlighting how these systems can either empower or further exclude vulnerable groups. It also provides recommendations for creating safer, more inclusive, and rights-based digital identification and verification systems.*

**Keywords:** *Data Privacy, Data Security, KYC, Marginalized Communities, Digital Inclusion, Financial Inclusion, Biometric Authentication, Data Protection, Vulnerable Populations, Digital Literacy*

### **INTRODUCTION:**

Data privacy and security have become critical global concerns as individuals increasingly rely on digital platforms for financial transactions, authentication, and government welfare access. Marginalized populations—such as migrant workers, rural communities, the urban poor, and undocumented individuals—face disproportionate risks because they often lack awareness, resources, or secure technological infrastructure.

KYC procedures, designed to prevent fraud and money laundering, require individuals to provide identity documents and personal data. While these systems are essential for security, they can unintentionally exclude vulnerable populations or expose them to privacy risks. This paper explores challenges, impacts, and solutions to ensure equitable, secure access.

### **DATA PRIVACY:**

Data privacy refers to an individual's right to control how their personal information is collected, used, stored, and shared. For marginalized groups, privacy violations may lead to surveillance, discrimination, and identity theft.

### **DATA SECURITY:**

Data security involves protecting digital information from unauthorized access, breaches, or misuse. Weak security systems put marginalized people at higher risk due to their limited ability to detect or respond to fraud.

### **KNOW YOUR CUSTOMER (KYC):**

KYC is a verification process used by banks, telecom providers, and digital platforms to confirm the identity of customers. KYC typically requires documents such as Aadhaar, PAN card, voter ID, or proof of residence—documents not always accessible to marginalized citizens.

### **MARGINALIZED COMMUNITIES:**

Groups that experience limited access to economic, social, or political resources, such as:

- Migrant laborers
- Homeless individuals
- Transgender persons
- Rural population without IDs
- Refugees and displaced communities

### **CHALLENGES AT THE INTERSECTION OF PRIVACY, SECURITY AND KYC**

#### **LACK OF DOCUMENTARY PROOF:**

Many marginalized individuals lack identity documents, making KYC compliance difficult. This results in exclusion from bank accounts, mobile SIM cards, and welfare programs.

### **DIGITAL ILLITERACY AND LACK OF AWARENESS:**

Low digital literacy increases vulnerability to fraud, phishing, and exploitation.

### **OVER-COLLECTION OF DATA:**

Some institutions require more data than necessary during KYC processes, exposing individuals to unnecessary privacy risks.

### **INSEURE STORAGE OF BIOMETRIC DATA:**

Biometric KYC (fingerprints, iris scans) carries the risk of irreversible damage if leaked, especially for individuals unable to defend legally.

### **LANGUAGE AND ACCESSIBILITY BARRIERS:**

Forms, apps, and verification systems may not be available in regional languages or accessible to persons with disabilities.

### **RISK OF EXCLUSION DUE TO TECHNOLOGY FAILURES:**

Biometric failures, network issues, or server downtime often deny services, to marginalized citizens who rely, on government benefits. Some institutions require more data than necessary during KYC processes, exposing individuals to unnecessary privacy risks.

### **IMPACT OF PRIVACY AND SECURITY ISSUES ON MARGINALIZED GROUP:**

- Financial exclusion
- Loss of welfare benefits
- Increased vulnerability to fraud
- Surveillance and discrimination
- Psychological stress and fear

### **GOVERNMENT AND INSTITUTIONAL INITIATIVES**

#### **AADHARR-BASED E-KYC:**

A fast and affordable method for identity verification, though challenges persist in biometric reliability.

### **RBI GUIDELINES ON VIDEO KYC:**

Video KYC reduces the need for physical documents and is helpful for the unbanked population.

### **DATA PROTECTION LAWS:**

India's Digital Personal Data Protection (DPDP) Act aims to protect personal data and define responsibilities of data fiduciaries.

### **FINANCIAL INCLUSION PROGRAMS:**

Schemes like PMJDY help vulnerable individuals obtain zero-balance accounts.

### **MINIMAL DATA COLLECTION:**

Institutions should collect only essential data required for basic verification.

### **STRENGTHENING DATA SECURITY FRAMEWORKS:**

- ❖ Encryption of sensitive information
- ❖ Regular audits
- ❖ Secure biometric systems

### **ALTERNATIVE KYC METHODS:**

- Offline e- KYC using QR-coded Aadhaar
- Social KYC (certification by local authorities)
- OTP-based verification for low-risk accounts

### **IMPROVING DIGITAL LITERACY:**

Community training programs can empower marginalized groups to detect fraud and protect their data.

### **CITIZEN – CENTRIC-PRIVACY DESIGN:**

Systems should be designed with transparency, consent-based data use, and multilingual support.

**BETTER ACCESSIBILITY:**

- Regional language apps
- Voice-based authentication
- Assistance centers in rural areas

**STRONG LEGAL SUPPORT:**

Clear grievance redressal mechanisms to protect victims of data breaches

**CONCLUSION:**

Data privacy, security, and KYC systems play a crucial role in shaping the financial and digital inclusion of marginalized communities. While these mechanisms aim to enhance trust and prevent fraud, poorly designed systems can deepen inequality. Ensuring that KYC processes are flexible, secure, and inclusive is essential for empowering vulnerable populations and protecting their rights in the digital era.

**REFERENCES:**

1. Digital Personal Data Protection Act (India), 2023.
2. Reserve Bank of India – KYC Master Directions.
3. World Bank – Digital Identification for Development (ID4D).
4. Reports on Financial Inclusion by NITI Aayog.

\*\*\*