Domain: Cryptography

Problem Statement: Privacy-Preserving KYC Verification System

Description

Design a privacy-preserving KYC verification system leveraging applied privacy-enhancing technologies (PETs), such as zero-knowledge proofs (ZKPs), that allows users to prove identity attributes (e.g., 'over 18', 'valid Aadhaar') without revealing sensitive personal identifiable information (PII).

Exact Deliverables

- Prototype of a privacy-preserving KYC system with user-friendly verification interfaces.
- Integration of selective-disclosure or zero-knowledge proof mechanisms.
- Performance benchmarking report comparing latency and usability against traditional e-KYC.
- Demonstration of compliance with India’s DPDP Act (2023) requirements.

Relevance

India executed more than 235 crore Aadhaar e-KYCs in FY24 alone. At this scale, privacy-first approaches are no longer optional but necessary. Breaches of KYC data can cause massive reputational and financial damage to organizations and individuals alike.

With the DPDP Act tightening regulations around consent and purpose limitation, industries handling customer data must urgently adopt privacy-preserving methods. Globally, regulatory trends in the EU, US, and Asia are converging towards privacy-first verification standards. An Indian innovation in this domain could become a model for privacy-preserving public digital infrastructure.

Business Case

Banks, NBFCs, fintechs, telecoms, and government agencies all rely on KYC verification. A privacy-preserving KYC solution reduces compliance risks, protects citizens' data, and builds trust with users. Additionally, it lowers the risk of fines and reputational harm from data breaches.

Such solutions could be deployed as middleware between Aadhaar e-KYC APIs and customer-facing apps, making them adoptable at scale without redesigning core systems. Globally, privacy-preserving verification systems are gaining traction, creating export opportunities for student-driven innovations.

Dataset(s)/Benchmarks

- Datasets: IBM AML-Data Synthetic Transactions Dataset, eKYC-DF Deepfake Dataset, UCI Adult Dataset
- Benchmarks: NIST FIPS-203/204 compliance, NIST SP 800-57

Milestones, Evolution Parameters

- Phase 1: Basic prototype with ZKP-based 'age over 18' verification.
- Phase 2: Expand to multi-attribute verification (e.g., address, Aadhaar validity).
- Phase 3: Integration with mock financial/telecom onboarding systems.
- KPIs: Verification latency vs. e-KYC, PII exposure reduction score, and user adoption experience (measured via mock testing).

Additional Information

- Benchmark systems against both Aadhaar e-KYC APIs and privacy-preserving identity protocols (e.g., Hyperledger Indy, W3C Verifiable Credentials).
- Focus on building usable, intuitive interfaces—privacy-preserving systems often fail due to poor UX.
- Systems must balance compliance with practicality; lightweight implementations that can scale are preferred.


इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते
www.isea.gov.in
DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative
CYBER SECURITY
INNOVATION CHALLENGE 1.0
DRIVING SECTOR-RELEVANT & FUTURE-READY CYBERSECURITY SOLUTIONS