RM 6201
Research Methodology

Academic Research Eco System: Case Studies
Module I-C

@ CSE/Maths, IIT Patna

Prof. Rajeev Kumar
Tech. & Edu.: Consultant & Policy
Ex-Prof. @ IITKgp, IITK, BITSP, JNU; Ex-DRDO Scientist
Rajeevkumar-cse.github.io

Include 3rd Party & LLM Generated Contents.

Feb. 2026

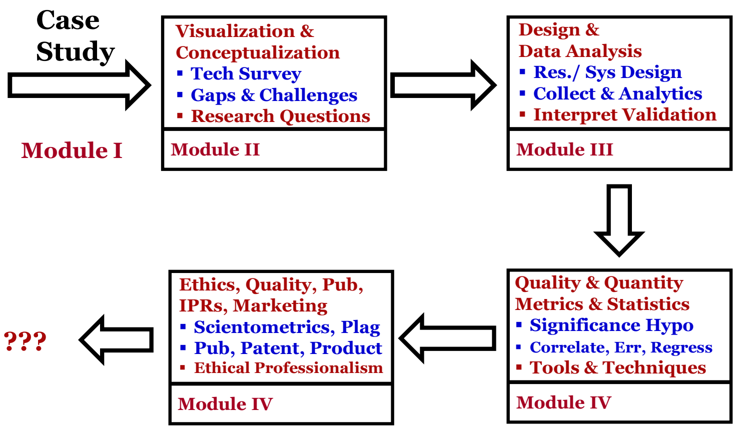
Objective?

**Make/Plan (?)
a ARE System**

What? | How? | Let us do it

ARES
System &
Case Studies

Overview : Making an ARES


Case Study

Module I

Visualization & Conceptualization
- Tech Survey
- Gaps & Challenges
- Research Questions

Module II

Design & Data Analysis
- Res./ Sys Design
- Collect & Analytics
- Interpret Validation

Module III

Quality & Quantity Metrics & Statistics
- Significance Hypo
- Correlate, Err, Regress
- Tools & Techniques

Module IV

Ethics, Quality, Pub, IPRs, Marketing
- Scientometrics, Plag
- Pub, Patent, Product
- Ethical Professionalism

Module IV

???

ResM: Case Study

Case Study

- ➔ Input ?
- ➔ ARES Modules II, III, IV, & V
- ➔ Output ?

➔ What to do?

➔ (Let us do)?

➔This Course?

Primality Testing: Primes in P?

- **How to work on**
  - Methodology
  - Methods
- . . .
- …

ARES: Case Studies

1. Primality Testing: Prime in P?

2. Digital Arrest ?

3. Digi Pers Data Protection ?

3. A Sub-System of OPERATION SINDOOR

4. <<< To be Added (TBA) >>>

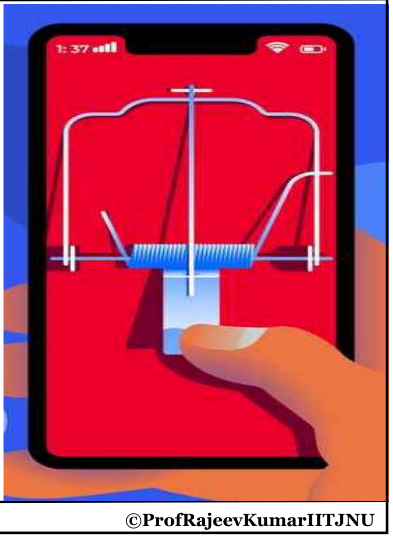
Case Study

Case: Digital Arrest

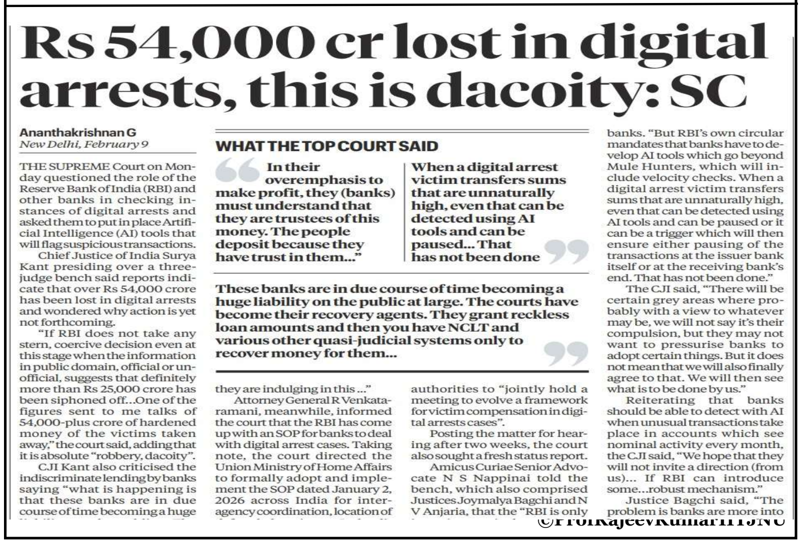
- ➔ Input ?
- ➔ Research ?
- ➔ Output ?
- **How to work on**
  - Methodology
  - Methods

➔ What to do?

➔This Course.



ARES: Digital Arrest; Feb 10, 2026: IndExpr



Rs 54,000 cr lost in digital arrests, this is dacoity: SC

Ananthakrishnan G
New Delhi, February 9

THE SUPREME Court on Monday questioned the role of the Reserve Bank of India (RBI) and other banks in checking instances of digital arrests and asked them to put in place Artificial Intelligence (AI) tools that will flag suspicious transactions.

Chief Justice of India Surya Kant presiding over a three-judge bench said reports indicate that over Rs 54,000 crore has been lost in digital arrests and wondered why action is yet not forthcoming.

"If RBI does not take any stern, coercive decision even at this stage when the information in public domain, official or unofficial, suggests that definitely more than Rs 25,000 crore has been siphoned off…One of the figures sent to me talks of 54,000-plus crore of hardened money of the victims taken away," the court said, adding that it is absolute "robbery, dacoity".

CJI Kant also criticised the indiscriminate lending by banks saying "what is happening is that these banks are in due course of time becoming a huge

WHAT THE TOP COURT SAID

> **In their overemphasis to make profit, they (banks) must understand that they are trustees of this money. The people deposit because they have trust in them..."**

> **When a digital arrest victim transfers sums that are unnaturally high, even that can be detected using AI tools and can be paused... That has not been done**

> **These banks are in due course of time becoming a huge liability on the public at large. The courts have become their recovery agents. They grant reckless loan amounts and then you have NCLT and various other quasi-judicial systems only to recover money for them...**

they are indulging in this ..."

Attorney General R Venkataramani, meanwhile, informed the court that the RBI has come up with an SOP for banks to deal with digital arrest cases. Taking note, the court directed the Union Ministry of Home Affairs to formally adopt and implement the SOP dated January 2, 2026 across India for inter-agency coordination, location of

authorities to "jointly hold a meeting to evolve a framework for victim compensation in digital arrests cases".

Posting the matter for hearing after two weeks, the court also sought a fresh status report.

Amicus Curiae Senior Advocate N S Nappinai told the bench, which also comprised Justices Joymalya Bagchi and N V Anjaria, that the "RBI is only

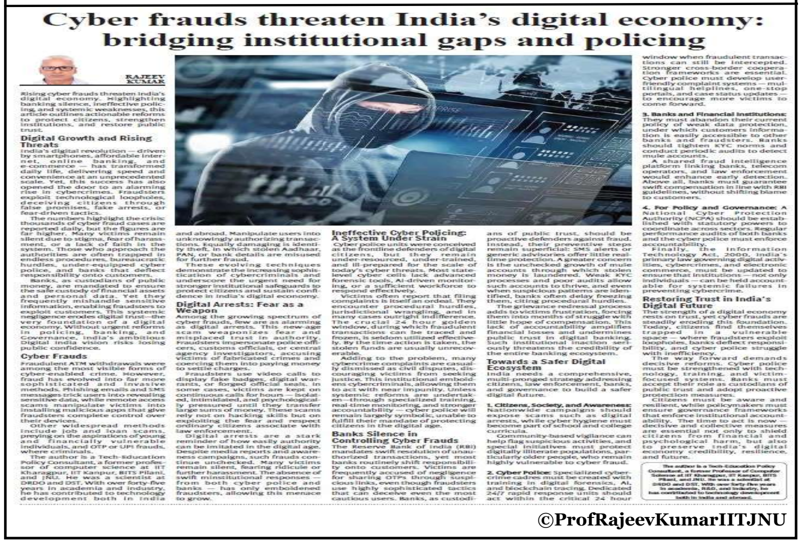
banks. "But RBI's own circular mandates that banks have to develop AI tools which go beyond Mule Hunters, which will include velocity checks. When a digital arrest victim transfers sums that are unnaturally high, even that can be detected using AI tools and can be paused or it can be a trigger which will then ensure either pausing of the transactions at the issuer bank itself or at the receiving bank's end. That has not been done."

The CJI said, "There will be certain grey areas where probably with a view to whatever may be, we will not say it's their compulsion, but they may not want to pressurise banks to adopt certain things. But it does not mean that we will also finally agree to that. We will then see what is to be done by us."

Reiterating that banks should be able to detect with AI when unusual transactions take place in accounts which see nominal activity every month, the CJI said, "We hope that they will not invite a direction (from us)... If RBI can introduce some...robust mechanism."

Justice Bagchi said, "The problem is banks are more into

Publishing: Sep 15, 2025: Pioneer



Cyber frauds threaten India's digital economy: bridging institutional gaps and policing

RAJEEV KUMAR

Rising cyber frauds threaten India's digital economy. Highlighting banking silence, ineffective policing, and systemic weaknesses, this article outlines actionable reforms to protect citizens, strengthen institutions, and restore public trust.

Digital Growth and Rising Threats

India's digital revolution — driven by smartphones, affordable internet, online banking, and e-commerce — has transformed daily life, delivering speed and convenience at an unprecedented scale. Yet, this success has also opened the door to an alarming rise in cybercrimes. Fraudsters exploit technological loopholes, deceiving citizens through false promises, fake arrests, or fear-driven tactics.

The numbers highlight the crisis: thousands of cyber fraud cases are reported daily, but the figures are far higher. Many victims remain silent due to stigma, fear of harassment, or a lack of faith in the system. Those who approach the authorities are often trapped in endless procedures, bureaucratic hurdles, under-equipped cyber police, and banks that deflect responsibility onto customers.

Banks, as custodians of public money, are mandated to ensure the safe custody of financial assets and personal data. Yet they frequently mishandle sensitive information, enabling fraudsters to exploit customers. This systemic negligence erodes digital trust—the very foundation of a digital economy. Without urgent reforms in policing, banking, and Governance, India's ambitious Digital India vision risks losing public confidence.

Cyber Frauds

Fraudulent ATM withdrawals were among the most visible forms of cyber-enabled crime. However, fraud has evolved into far more sophisticated and invasive methods. Phishing emails and SMS messages trick users into revealing sensitive data, while remote access scams manipulate victims into installing malicious apps that give fraudsters complete control over their devices.

Other widespread methods include job and loan scams, preying on the aspirations of young and financially vulnerable individuals, and OTP or UPI frauds, where criminals

The author is a Tech-Education Policy Consultant, a former professor of computer science at IIT Kharagpur, IIT Kanpur, BITS Pilani, and JNU. He was a scientist at DRDO and DST. With over forty-five years in academia and industry, he has contributed to technology development both in India

and abroad. Manipulate users into unknowingly authorizing transactions. Equally damaging is identity theft, in which stolen Aadhaar, PAN, or bank details are misused for further fraud.

These evolving techniques demonstrate the increasing sophistication of cybercriminals and underscore the urgent need for stronger institutional safeguards to protect citizens and sustain confidence in India's digital economy.

Digital Arrests: Fear as a Weapon

Among the growing spectrum of cyber frauds, few are as alarming as digital arrests. This new-age scam weaponizes fear and misplaced trust in authority. Fraudsters impersonate police officers, customs officials, or central agency investigators, accusing victims of fabricated crimes and coercing them into paying money to settle charges.

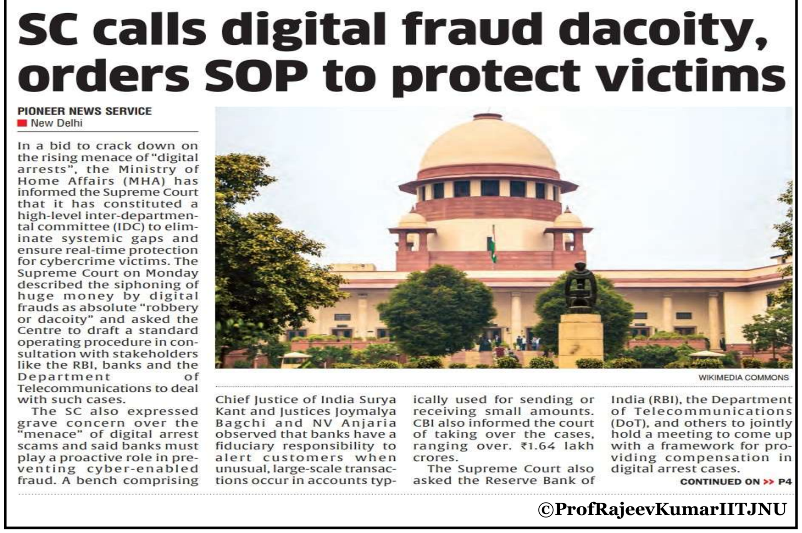
Fraudsters use video calls to display fake badges, digital warrants, or forged official seals. In some cases, victims are kept on continuous calls for hours — isolated, intimidated, and psychologically pressured until they transfer large sums of money. These scams rely not on hacking skills but on exploiting the fear and respect ordinary citizens associate with law enforcement.

Digital arrests are a stark reminder of how easily authority can be imitated in the digital age. Despite media reports and awareness campaigns, such frauds continue unchecked. Many victims remain silent, fearing ridicule or further harassment. The absence of swift minstitutional responses — from both cyber police and banks — has only emboldened fraudsters, allowing this menace to grow.

Ineffective Cyber Policing: A System Under Strain

[illegible]

ARES: Digital Arrest : Feb. 10, 2026; Pioneer



SC calls digital fraud dacoity, orders SOP to protect victims

PIONEER NEWS SERVICE
New Delhi

In a bid to crack down on the rising menace of "digital arrests", the Ministry of Home Affairs (MHA) has informed the Supreme Court that it has constituted a high-level inter-departmental committee (IDC) to eliminate systemic gaps and ensure real-time protection for cybercrime victims. The Supreme Court on Monday described the siphoning of huge money by digital frauds as absolute "robbery or dacoity" and asked the Centre to draft a standard operating procedure in consultation with stakeholders like the RBI, banks and the Department of Telecommunications to deal with such cases.

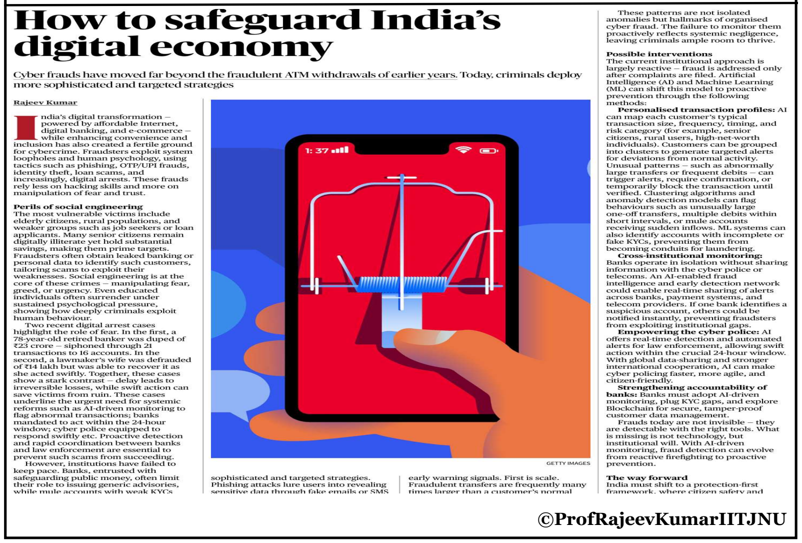
WIKIMEDIA COMMONS

The SC also expressed grave concern over the "menace" of digital arrest scams and said banks must play a proactive role in preventing cyber-enabled fraud. A bench comprising Chief Justice of India Surya Kant and Justices Joymalya Bagchi and NV Anjaria observed that banks have a fiduciary responsibility to alert customers when unusual, large-scale transactions occur in accounts typically used for sending or receiving small amounts. CBI also informed the court of taking over the cases, ranging over. ₹1.64 lakh crores.

The Supreme Court also asked the Reserve Bank of India (RBI), the Department of Telecommunications (DoT), and others to jointly hold a meeting to come up with a framework for providing compensation in digital arrest cases.

CONTINUED ON >> P4

Publishing : Oct 03, 2025: Hindu



How to safeguard India's digital economy

Cyber frauds have moved far beyond the fraudulent ATM withdrawals of earlier years. Today, criminals deploy more sophisticated and targeted strategies

Rajeev Kumar

India's digital transformation – powered by affordable Internet, digital banking, and e-commerce – while enhancing convenience and inclusion has also created a fertile ground for cybercrime. Fraudsters exploit system loopholes and human psychology, using tactics such as phishing, OTP/UPI frauds, identity theft, loan scams, and increasingly, digital arrests. These frauds rely less on hacking skills and more on manipulation of fear and trust.

Perils of social engineering

The most vulnerable victims include elderly citizens, rural populations, and weaker groups such as job seekers or loan applicants. Many senior citizens remain digitally illiterate yet hold substantial savings, making them prime targets. Fraudsters often obtain leaked banking or personal data to identify such customers, tailoring scams to exploit their weaknesses. Social engineering is at the core of these crimes – manipulating fear, greed, or urgency. Even educated individuals often surrender under sustained psychological pressure, showing how deeply criminals exploit human behaviour.

Two recent digital arrest cases highlight the role of fear. In the first, a 78-year-old retired banker was duped of ₹23 crore – siphoned through 21 transactions to 16 accounts. In the second, a lawmaker's wife was defrauded of ₹14 lakh but was able to recover it as she acted swiftly. Together, these cases show a stark contrast – delay leads to irreversible losses, while swift action can save victims from ruin. These cases underline the urgent need for systemic reforms such as AI-driven monitoring to flag abnormal transactions; banks mandated to act within the 24-hour window; cyber police equipped to respond swiftly etc. Proactive detection and rapid coordination between banks and law enforcement are essential to prevent such scams from succeeding.

However, institutions have failed to keep pace. Banks, entrusted with safeguarding public money, often limit their role to issuing generic advisories, while mule accounts with weak KYCs

GETTY IMAGES

sophisticated and targeted strategies. Phishing attacks lure users into revealing sensitive data through fake emails or SMS

early warning signals. First is scale. Fraudulent transfers are frequently many times larger than a customer's normal

These patterns are not isolated anomalies but hallmarks of organised cyber fraud. The failure to monitor them proactively reflects systemic negligence, leaving criminals ample room to thrive.

Possible interventions

The current institutional approach is largely reactive – fraud is addressed only after complaints are filed. Artificial Intelligence (AI) and Machine Learning (ML) can shift this model to proactive prevention through the following methods:

Personalised transaction profiles: AI can map each customer's typical transaction size, frequency, timing, and risk category (for example, senior citizens, rural users, high-net-worth individuals). Customers can be grouped into clusters to generate targeted alerts for deviations from normal activity. Unusual patterns – such as abnormally large transfers or frequent debits – can trigger alerts, require confirmation, or temporarily block the transaction until verified. Clustering algorithms and anomaly detection models can flag behaviours such as unusually large one-off transfers, multiple debits within short intervals, or mule accounts receiving sudden inflows. ML systems can also identify accounts with incomplete or fake KYCs, preventing them from becoming conduits for laundering.

Cross-institutional monitoring: Banks operate in isolation without sharing information with the cyber police or telecoms. An AI-enabled fraud intelligence and early detection network could enable real-time sharing of alerts across banks, payment systems, and telecom providers. If one bank identifies a suspicious account, others could be notified instantly, preventing fraudsters from exploiting institutional gaps.

Empowering the cyber police: AI offers real-time detection and automated alerts for law enforcement, allowing swift action within the crucial 24-hour window. With global data-sharing and stronger international cooperation, AI can make cyber policing faster, more agile, and citizen-friendly.

Strengthening accountability of banks: Banks must adopt AI-driven monitoring, plug KYC gaps, and explore Blockchain for secure, tamper-proof customer data management.

Frauds today are not invisible – they are detectable with the right tools. What is missing is not technology, but institutional will. With AI-driven monitoring, fraud detection can evolve from reactive firefighting to proactive prevention.

The way forward

India must shift to a protection-first framework, where citizen safety and

Types of Methodologies in CSE:

Paradigms

- **Analytical**
- **Algorithmic**
    - Deterministic
    - Approximation
    - Stochastic
    - Hybrid . . .
- **Empirical: Experimental**
- **Statistical & Probabilistic**
- **Combinations**

Types of Systems

- **Manual / Conventional**
- **Mechanized**
- **Semi-Autonomous**
- **Autonomous**
- **Assisted Tech.**
- **IoT Enabled : Smart**
- **AI/ML Enabled : Intelligent**

Types of Methodologies in CSE:

- **Types of Solutions**
    - Optimal / Near-Optimal
    - Accurate
    - Approximate
    - Probabilistic
    - . . .
- **Algorithmic Complexity**
- **Time Bounds: limits**
- **…**

Question ?

Feedback ?