# THE ROLE OF FORENSIC ACCOUNTING IN REDUCING SYSTEMIC RISK WITHIN INDIA'S DIGITAL PUBLIC INFRASTRUCTURE: AN ANALYTICAL STUDY OF UPI, ULI AND CBDC

Saptarshi Datta*

Dr. Himanshu D. Thakkar**

## Abstract

The shift in India's financial infrastructure is driven by the rapid growth and development of its Digital Public Infrastructure (DPI). This includes Unified Payments Interface (UPI) payment systems, the Unified Lending Interface (ULI) lending platform concept and pilot tests for Central Bank Digital Currency (CBDC). These innovations have improved transaction speed and enhanced financial inclusion. However, alongside the benefits of new computerized banking systems, digitalization in banking has also increased the risk of sophisticated cyber-enabled financial crimes. As a result, traditional post hoc methods are becoming less effective. To address these challenges, forensic accounting methodology has been used to examine systemic risks, operational vulnerabilities and cyber security issues associated with these new payment methods. The study uses secondary data from the National Payments Corporation of India (NPCI). This data concerns transaction volume and usage by participating institutions. The analysis focuses on transaction volume and the total downtime of the infrastructure utilized by participating banks. The results indicate an urgent need to design an architecture that incorporates Forensic Accounting. The paper suggests that employing real-time data analytics, continuous anomaly detection and embedded digital forensics will help protect the integrity of fiscal operations. Additionally, recommended the need for suitable regulatory actions.

**Keywords**

Forensic Accounting, Unified Payments Interface (UPI), Unified Lending Interface (ULI), Central Bank Digital Currency (CBDC), Cyber Security, Fraud Analytics

## Introduction

### *The Macroeconomic Paradigm Shift in Digital Public Infrastructure*

India is currently experiencing a structural and epistemological transformation in the architecture of its financial system. Emerging market economies have historically faced frictional costs associated with cash-based operations, including high cash-to-Gross Domestic Product (GDP) ratios, leakage from unrecorded economic activities and barriers to financial inclusion. However, the aggressive expansion of India's Digital Public Infrastructure (DPI), built on foundational layers of identity (Aadhaar) and telecommunications, has fundamentally remapped the country's financial landscape.

The key factors that influence this new environment are the New Avenues for Payment Systems. The evolution of payment systems has become a complex combination of three separate payment systems: UPI, ULI and Central Bank Digital Currency (CBDC). Each payment system has been created with a specific purpose in the macroeconomic

*UG Research Scholar, School of Management Studies, National Forensic Sciences University.
**Assistant Professor, School of Management Studies, National Forensic Sciences University.

framework. UPI has created tremendous scale and democratised retail and Peer-to-Peer (P2P) transfers. ULI is poised to transform the way credit is delivered to customers, eliminating the information asymmetries that have prevented adequate funding for Micro, Small and Medium Enterprises (MSMEs) in the past and using algorithms to aggregate data for lenders, thereby, enabling frictionless lending. At the same time, CBDC (the e₹) was introduced as the sovereign solution to the decentralisation of digital assets, providing an institutionally backed electronic currency that is immutable and programmable and eliminating inter-bank settlement risk.

While all of these platforms provide unmatched operational efficiency and have significantly accelerated the formalisation of the economy as a whole, they create a paradoxical risk. As the time required to complete a transaction approaches zero, there will be less and less time to identify, interrupt and mitigate fraud in the financial system.

***The Topology of Systemic Risk and Cyber-Enabled Financial Crime***

The hyper-digitalisation of banking has dramatically changed the attack surface that cyber criminals target. Where physical fraud was limited by location, document verification and lengthy processing times/ transaction clearance processes in older banks, with digital money transfers, these constraints have been effectively removed. This means the "Fraud Triangle" (Opportunity/Pressure/Rationalisation) of fraud now exists entirely within the cyberspace domain.

Historically, the threats to banks were typically beyond their control, whereas, those created by today's banking systems are systemic. For example, according to recent data, the volume of UPI transactions is enormous, creating a complex environment where criminals can easily hide their attempts at micro-structuring and fast routing through complex networks of money mule accounts. In addition, phishing, application spoofing and Application Programming Interface (API) endpoint impersonation have become standard operating procedures.

As ULI continues to grow rapidly, the risk of synthetic identity fraud will increase. Since ULI requires financial institutions to aggregate multiple digital footprints (e.g. digitised land registrations, Goods and Service Tax (GST) returns and alternative banking sources), the integrity of the data silos that underpin lending, in this regard, is becoming a critical vulnerability for financial institutions. If a threat actor can manipulate or intercept the API data flow, they can algorithmically exploit the system to generate unsecured and irrecoverable debt. Similarly, while the distributed ledger technology underlying CBDC architectures is mathematically robust, the vulnerability shifts to the retail endpoints-specifically, cryptographic key theft and digital wallet exploits. These complex threat vectors represent a convergence of cyber-intrusions and economic exploitation, creating a risk landscape that threatens the fiscal integrity of the broader banking system.

***The Inadequacy of Traditional Auditing and the Epistemological Shift***

Conventional audit methods used for governance auditing have thus become outdated due to the increasing number and complexity of high-technology threats. Traditional financial governance audits are retrospective, static and use sampling techniques; therefore, these audits generally rely on end-of-business-day account reconciliations and analyses of events that occurred before the audit. Consequently, the typical audit process will not detect a discrepancy or an unauthorised fund transfer conducted using a real-time gross settlement system for some time after those funds have moved illegally through multiple jurisdictions and been converted into indistinguishable assets.

To address systemic latency, financial institutions need an epistemological shift in how they approach compliance enforcement and asset protection. Specifically, there needs to be a shift from reactive auditing to proactive enforcement via a variety of defence mechanisms. Forensic accounting can illustrate its benefit in this area.

Forensic accounting is more than just confirming the accuracy of financial records; rather, it represents a new approach to accounting, as an interdisciplinary science through which such things as investigative accounting can be integrated with econometric modelling techniques, investigating legal frameworks and using sophisticated technology and digital data analytic techniques to analyse the available information. Forensic accounting provides analytical tools needed to investigate Electronic Funds Transfer (EFT) activity within India. EFT transactions can be analysed using various methods, such as statistically examining the distribution of large transaction datasets under Benford's Law. In addition to statistical analysis, credit applications may also be reviewed for unusual behaviour patterns using machine-learning tools and tracing systems (blockchain), which will allow for creating a map of the transaction flow of programmable digital currencies and CBDCs.

***The Concept of Forensic-by-Design***

This paper proposes that, for India to secure its digital future, simply overlaying security protocols on existing systems will not suffice; it is necessary to create a "Forensic-by-Design" structure across the ecosystem. The ecosystem must have the capability to include continuous control monitoring APIs, automated anomaly-detection triggers and digital evidence preservation protocols, natively hard-coded into the foundational switching layers of UPI, ULI and CBDC networks. By incorporating forensic methodologies into the payment infrastructure, financial institutions can shift their focus from an investigative to a deterministic/preventative model.

**Literature Review**

The academic discourse surrounding the Digital Public Infrastructure (DPI) has historically been divided into two distinct streams: macroeconomic studies focusing on financial inclusion and purely technical literature detailing cryptographic protocols. However, a critical interdisciplinary gap persists in applying forensic accounting methodologies to real-time and high-velocity digital payment systems. This review synthesises the prevailing literature across UPI, ULI and CBDC ecosystems to establish a conceptual foundation for Forensic-by-Design architectures.

***The Operational Efficacy and Systemic Risks of the Unified Payments Interface (UPI)***

The Unified Payments Interface (UPI) has been extensively described in the literature as a facilitator of the disintermediation of retail payments. Many of the foundational papers describing India's DPI highlight how the interoperable API switches that allow users to access and transfer fiat to one another immediately are architecturally beautiful (Jaison P et al., 2026). However, recent studies in criminology and financial security highlight a dark complement to resistance-free payment systems: the industrialisation of cyber-enabled crimes against financial institutions (Chinkhando Banda et al., 2025).

Current literature identifies that the "friction" of the traditional banking system, such as clearing house delays and the need for a person to verify the signature of the person attempting to deposit a physical check, functioned as an effective security measure on its own (Thakkar et al., 2025). With UPI, that "friction" is essentially zero, as it settles in milliseconds, effectively eliminating any time for the victim of traditional fraud to intervene.

The cyber security community in digital payments has noted that the source of threat vectors has shifted from complex algorithmic hacking to scalable social engineering approaches that utilise techniques such as application spoofing, SIM swapping and automated phishing payloads. Scholars have also noted that there is a proliferation of "mule account" networks (Rabha & Chourasia, 2025), which interests malicious actors who take advantage of the asymmetrical Know Your Customer (KYC) compliance standards across various regional and co-operative banks, allowing the malicious actor to transfer value through a variety of different intermediaries (Thakkar et al., 2025). As a result of the traditional auditing process's reliance on periodic sampling, it is empirically incapable of detecting these micro-structuring techniques, necessitating

a shift from periodic assessments of the legitimacy of transactions to the use of real-time forensic data analytics to monitor the movement of illicit funds within banking networks (Sateesh Kumar et al., 2025). Forensic accountants face many challenges, such as international collaboration issues, utilization of advanced forensic data analytics, ethical leadership, etc. (Dimitropoulos & Reading, 2025)

***Unified Lending Interface (ULI) and the Emergence of Synthetic Identity Fraud***

The transition of the ecosystem from payment facilitation to seamless delivery of credit through the Unified Lending Interface (ULI) demonstrates a fundamental change in systemic risk as found in the existing literature. ULI, which operates under the Open Credit Enablement Network (OCEN), is focused on algorithmically approving credit based on multiple disparate sources of secondary data (e.g. digitised land records, GST returns and alternative banking histories) (Chidipothu et al., 2026).

The risk of synthetic identity fraud and data contamination is significant in financial risk literature and in an automated lending environment, a cyber criminal can manipulate streams of data from an Application Programming Interface (API) to create a synthetic legitimate borrower profile based on a series of fragmented or stolen pieces of identity (Dattatreya Murthy, 2026). Recent studies into open banking frameworks has identified the risk of credit circularity associated with unverified microloans being continually rolled over among different lending platforms by manipulating the digital footprint of the borrower, making that footprint appear current; as related to banking, risk between platforms is a high level of risk (Thakkar et al., 2025). In forensic accounting, the academic literature identifies static historical KYC documentation lacks holistic view of customer in a ULI-based environment (Sampathkumar et al., 2026). Academics recommend implementing behavioural biometric and predictive forensic modelling to validate the authenticity of the data stream prior to credit generation, a concept quantitatively tested in this paper by analysing downtime vulnerability (Thakkar et al., 2024).

***Central Bank Digital Currency (CBDC): Architectural Resilience and Endpoint Vulnerabilities***

The introduction of Central Bank Digital Currencies (CBDCs) is opening up a new type of cryptographic opportunity. Several studies on CBDC deployment (such as the digital RMB and the Sand Dollar) have focused on the "Anonymity vs. Traceability" problem (Ghosh & Das 2026). Many of the working papers published by central banks discuss the fact that while Distributed Ledger Technology (DLT) maintains the integrity and security of the data contained in a CBDC, there is very little that can be done to reduce the risk that cyber crime will occur within a CBDC ecosystem (Thakkar et al., 2024).

Most of the cyber security literature on digital currencies clearly distinguishes between attacks on ledgers and cyber-attacks on endpoints. The CBDC network itself is designed to withstand centralised attacks, while the user-facing retail digital wallets are vulnerable to key theft, malware injection and smart contract exploits. Costly forensic analyses of blockchain environments have demonstrated that it is extremely difficult to trace programmable currencies after they have been laundered through a decentralized mixer or through the dark web (Brühl, 2026). The consensus among experts on securing a CBDC is that advanced digital forensic techniques, such as automated algorithmic tracing tools capable of mapping complex blockchain networks, will assist law enforcement agencies in investigating digital currency crime without violating the privacy rights of legitimate users (Desai & Bhatt, 2025).

***The Paradigm Shift: From Retrospective Audit to Continuous Control Monitoring (CCM)***

The standard audit method cannot keep up with the new forms of digital payment. Traditional audits are based on historical records of transactions settled after the fact, generally requiring an assessment of the dollar amount involved and a reference to records maintained by the entity, which are typically reviewed manually. These audit requirements do not align with current digital payment practices (Hoti et al., 2025).

Current forensic accounting papers generally recommend that accounting bodies immediately shift to Continuous Control Monitoring (CCM). Under CCM, automated scripts and forensic algorithms will be incorporated directly into financial institutions' information technology infrastructures. Various studies have shown that using statistical anomalies, such as Benford's Law, can detect patterns of clustering and automation in very high-volume and fast-moving electronic payments data (Wang et al., 2026). Many sources state that machine-learning-based anomaly detection systems are critically important for developing and maintaining baseline behaviours of user accounts and will trigger immediate forensic transactions suspension when deviations occur (Correia, 2026).

**Research Objectives and Scope of the Study**

This study examines India's new payment system architecture to assess its structural resilience. This study is based solely on secondary empirical data obtained from the Reserve Bank of India (RBI), the National Payments Corporation of India (NPCI) and the Indian Computer Emergency Response Team (CERT-In). To accomplish its goals, the study is organized around four principal objectives:

- The quantitative evaluation of the loads placed upon and the adoption rates of the UPI, ULI and CBDC payment ecosystems by examining and analyzing historical empirical data between 2025 and 2026.
- The discovery and mapping of cyber security vulnerabilities and operational constraints associated with high-velocity payments.
- The analysis of the effectiveness of forensic accounting methods — specifically continuous-control monitoring and predictive-data analysis — at mitigating synthetic identity fraud, transaction laundering and endpoint exploits.
- The development of a structural and regulatory framework — Forensic - by - Design — for banking institutions to incorporate proactive investigative mechanisms into their digital public infrastructure.

By addressing the objectives stated above, this study will advance the emerging field of forensic economics and provide actionable policy guidance to banking industry professionals, regulatory authorities and law enforcement agencies responsible for ensuring the security and integrity of the nation's payment systems.

**Research Methodology**

This study adopts a descriptive-analytical research design that utilises secondary data to assess the operational landscape of India's payment systems.

Data Sources: The primary datasets were extracted from the National Payments Corporation of India (NPCI) official statistics, specifically focusing on product statistics and downtime reports for the fiscal year 2025-2026.

Variables Analysed: Transaction volume (in millions), transaction value (in ₹ Crores), ecosystem participation (number of live banks) and system downtime incidents/duration.

Analytical Framework: The empirical data is subjected to specific analytical techniques mapped directly to the study's core objectives; the Trend Analysis is applied to the transaction volume and value datasets to address Objective 1 (quantitative evaluation of ecosystem loads). Pareto Analysis is utilised for system downtime incidents to address Objective 2 (discovery and mapping of operational constraints and vulnerabilities). Finally, the identified systemic pressure points are evaluated through a Forensic Risk-Assessment Matrix to address Objectives 3 and 4, enabling the analysis of forensic mitigation strategies and the development of the Forensic-by-Design framework.

**Analysis and Findings**

The foundational premise of forensic analytics in digital payments relies on understanding the scale and stress points of the infrastructure.

***Transaction Velocity and Ecosystem Stress***

The explosive growth of UPI creates a massive,

continuous dataset. For forensic accountants, this volume represents both a challenge (data fatigue) and an opportunity (rich datasets for machine learning-based anomaly detection).

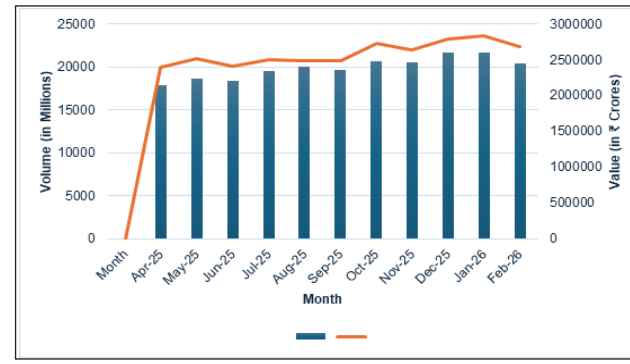
**Table 1: UPI Monthly Transaction Volume and Value**

| Month | Volume (in Mn.) | Average Daily Volume (in Mn.) | Value (in ₹ Cr.) | Average Daily Value (in ₹ Cr.) |
|---|---|---|---|---|
| March-2026 | 11,187.14 | 745.81 | 1,508,868.86 | 100,591.26 |
| February-2026 | 20,394.20 | 728.36 | 2,684,229.30 | 95,865.33 |
| January-2026 | 21,703.46 | 700.11 | 2,833,481.26 | 91,402.62 |
| December-2025 | 21,634.67 | 697.89 | 2,796,712.71 | 90,216.54 |
| November-2025 | 20,466.98 | 682.23 | 2,631,632.64 | 87,721.09 |
| October-2025 | 20,700.92 | 667.77 | 2,727,790.71 | 87,993.25 |
| September-2025 | 19,633.43 | 654.45 | 2,489,736.52 | 82,991.22 |
| August-2025 | 20,008.31 | 645.43 | 2,485,472.90 | 80,176.55 |
| July-2025 | 19,467.95 | 628.00 | 2,508,498.10 | 80,919.29 |
| June-2025 | 18,395.01 | 613.17 | 2,403,930.69 | 80,131.02 |
| May-2025 | 18,677.46 | 602.50 | 2,514,297.01 | 81,106.35 |
| April-2025 | 17,893.42 | 596.44 | 2,394,925.87 | 79,830.86 |

Source: Compiled by the Author based on National Payments Corporation of India (NPCI) official statistics (2025-2026)

The Unified Payments Interface (UPI) is a digital payment platform that enables instant payments between two users via their respective banks. Table 1 presents monthly UPI transaction metrics for each calendar month from April 2025 to March 2026. The magnitude of UPI's digital transformation can be gauged by the peak monthly transaction volume in January 2026, which exceeded 21.7 billion UPI transactions. Additionally, these total transaction volumes, when viewed from a forensic accounting perspective, create an unparalleled amount of data requiring processing; existing audit methodologies, which are based on sampling less than one percent of total transactions, are incapable of providing significant levels of audit assurance due to the volume of data that would have to be reviewed. To maintain ongoing audit assurances, banks will need to adopt fully automated, high-volume, big-data analytics to monitor the integrity of their ledger systems continuously.

**Figure 1: Dual-Axis Trend of Volume vs. Value**




Source: Compiled by Author

According to Figure 1, the Temporal Trajectory of UPI Adoption exhibits a strong volume-value asymmetry. All data points indicate that both volume and value are trending upward; however, the visual asymmetry suggests that the financial system is significantly more weighted towards high-frequency and low-value transactions than towards low-frequency

and high-value transactions. This visual trend line is directly correlated with the camouflage used by forensic investigators during source-and-method analysis to determine whether Micro Structuring or Smurfing operations have occurred. The graph shows how destructive actors can potentially distribute a substantial amount of illicit cash through Dollars at License (DALC). By leveraging the sheer velocity of retail microtransactions, a destructive actor may completely bypass any value limits established by legacy Anti-Money Laundering (AML) criteria.

***Ecosystem Expansion and Security Disparities***

As the number of participating banks increases, the variance in internal cyber security standards widens. A single compromised bank API can serve as a conduit for systemic attacks.

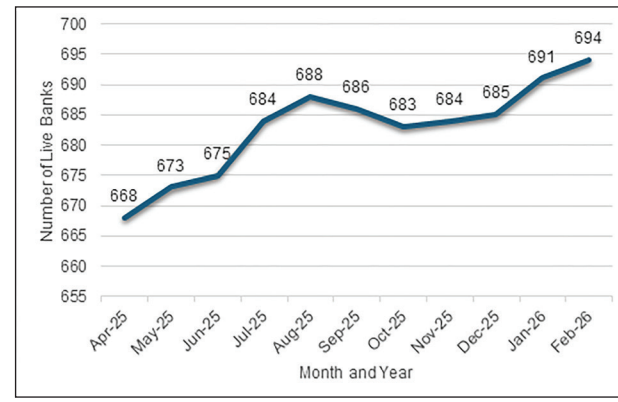
**Table 2: Ecosystem Growth - Banks Live on UPI**

| Month | No. of Banks live on UPI | Month-Over-Month Change | Forensic Risk Implication |
|---|---|---|---|
| February-2026 | 694 | +3 | Expanding API endpoint attack surface |
| January-2026 | 691 | +6 | Increased need for endpoint standardization |
| December-2025 | 685 | +1 | Stable ecosystem mapping |
| November-2025 | 684 | +1 | Stable ecosystem mapping |
| October-2025 | 683 | -3 | Potential de-registrations/mergers |
| September-2025 | 686 | -2 | System consolidation |
| August-2025 | 688 | +4 | Rapid regional bank onboarding |
| July-2025 | 684 | +9 | High risk of non-compliant API integration |
| June-2025 | 675 | +2 | Steady growth |
| May-2025 | 673 | +5 | Steady growth |
| April-2025 | 668 | Base | Baseline |

Source: Compiled by Author based on National Payments Corporation of India (NPCI) official statistics (2025-26)

Table 2 tracks month-by-month growth in the integration of financial institutions on the UPI network, resulting in 694 banks now live. This integration reflects the structural de-centrality of the payments architecture in India. The table illustrates a growing disparity in IT budgets and internal audit capabilities between these newly integrated institutions and other regional, co-operative and payments banks as they transition to UPI's centralised infrastructure. In summary, this numerical growth demonstrates the systemic need for standardised, mandated security compliance to ensure that newly onboarded institutions will not adversely affect the integrity of the broader network.

**Figure 2: Expansion Trajectory of Participating Banks**




Source: Compiled by Author

Figure 2, an area chart, represents the growing attack surface for the UPI ecosystem. The area under the trendline is a visual representation of the "API Endpoint Risk" to the network. As the ecosystem's visual footprint expands, the likelihood of a cyber-intrusion increases due to a less secure node. The visualisation supports the forensic premise that digital public infrastructure is only as resilient as its least well-integrated endpoint; therefore, continuous perimeter stress testing should be conducted across all entities in the ecosystem.

***Operational Vulnerabilities: Downtime as a Forensic Indicator***

System downtime is not merely a technical glitch; from a forensic viewpoint, it is a critical vulnerability window. Outages disrupt reconciliation, creating blind spots where malicious transactions can bypass real-time monitoring.

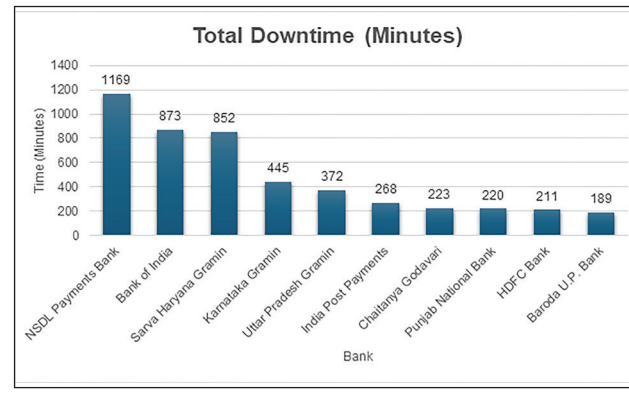
**Table 3: Technical Downtime Analysis by Member Banks (February 2026)**

| Sr. No. | Name of the Member Bank | Incident Count | Downtime (Hours: Minutes) | Forensic Classification |
|---|---|---|---|---|
| 1 | NSDL Payments Bank Limited | 5 | 19:29 | Critical Vulnerability Node |
| 2 | Bank of India | 3 | 14:33 | High Risk |
| 3 | Sarva Haryana Gramin Bank | 1 | 14:12 | High Risk |
| 4 | Karnataka Gramin Bank | 1 | 07:25 | Moderate Risk |
| 5 | Uttar Pradesh Gramin Bank | 1 | 06:12 | Moderate Risk |
| 6 | India Post Payments Bank | 4 | 04:28 | Recurring Instability |
| 7 | Chaitanya Godavari Grameen Bank | 1 | 03:43 | Low-Moderate Risk |
| 8 | Punjab National Bank | 4 | 03:40 | Recurring Instability |
| 9 | HDFC Bank | 1 | 03:31 | Low Risk |
| 10 | Baroda U.P. Bank | 1 | 03:09 | Low Risk |
| 11 | Central Bank of India | 2 | 01:50 | Low Risk |
| 12 | IndusInd Bank | 1 | 01:20 | Minimal Risk |
| 13 | Indian Overseas Bank | 1 | 00:33 | Minimal Risk |

Source: Compiled by Author based on National Payments Corporation of India (NPCI) official statistics (2025-26)

Table 3 presents technical downtime metrics for a sample of member banks, showing that the level of infrastructure capability differs significantly across banks. In particular, payment institutions (also known as payments banks) and regional rural banks experience significantly higher downtime than other banks; for example, NSDL Payments Bank recorded more than 19 hours of downtime in February 2026. Looking at this from a forensic perspective, these minute-by-minute records of downtime are significant weaknesses, as they indicate specific times when automated reconciliation cannot occur, when real-time transaction-monitoring systems are offline and when there are no records in the digital ledger.

**Figure 3: Analysis of System Downtime (February 2026)**




Source: Compiled by Author

In Figure 3, the downtime data is examined to provide a visual representation of the severity of the structural asymmetry observed in the organisation's network operational resiliency. The cumulative percentage line suggests that approximately 80% of the instability caused across multiple systems can be attributed to a very small number of institutions in the network. Forensic accountants and IT auditors will use this chart as a prioritisation matrix during their audits. Regulatory audits and digital forensics resources should be closely focused on these nodes with high levels of downtime to limit their potential to serve as unauthorised access channels for cyber-enabled financial fraud.

**Integrating ULI and CBDC: The Next Frontier of Financial Crime**

While the empirical data above highlight the pressures on existing infrastructure, the imminent scaling of ULI and CBDC introduces complex new threat vectors.

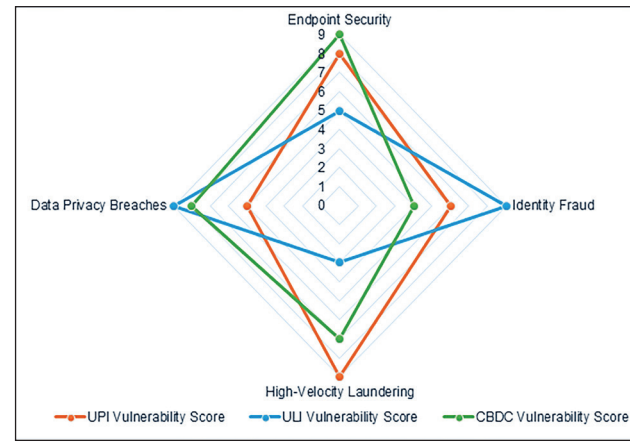
**Table 4: Comparative Threat Topology across DPI Avenues**

| Payment System | Primary Architecture | Core Forensic Risk Area | Prevailing Cyber Threat Vectors |
|---|---|---|---|
| UPI | Centralized Switch, API-driven | Transaction Laundering, Mule Accounts | App Spoofing, Phishing, SIM Swapping |
| ULI | Decentralized Data Aggregation | Synthetic Identity Fraud, Credit Layering | Credential Stuffing, API Data Interception |
| CBDC | Distributed Ledger Technology | Endpoint Compromise, Smart Contract Logic Flaws | Cryptographic Key Theft, Wallet Exploits |

Source: Compiled by Author

Table 4 lists multiple risk vectors related to UPI, ULI and CBDC. Each architecture is assigned a vulnerability score based on a 10-point forensic risk scale, where 1 indicates minimal systemic threat and 10 indicates a critical, highly probable vulnerability requiring immediate intervention. Based on this framework, UPI exhibits a high vulnerability to high-velocity laundering (Score: 9/10), ULI shows critical risks regarding identity fraud (Score: 9/10) and CBDC demonstrates severe vulnerability to endpoint security compromises (Score: 9/10). Therefore, it can be concluded that no single security protocol can be used for all financial institutions; instead, individual forensic interventions are required for each financial institution's unique infrastructure.

**Figure 4: Forensic Focus Distribution Matrix**




Source: Compiled by Author

The chart in Figure 4 presents a multidimensional view of how to approach forensics differently for different payment types. Each of the unique shapes—UPI, ULI and CBDC—depicts that the

same types of threats are likely to evolve based on the underlying technology. In fact, while CBDC protects the master ledger (absorbing risk on the anti-money laundering axis), it increases endpoint security risk. This makes this chart an essential tool for a Chief Information Security Officer (CISO) when designing a flexible and layered forensic defence architecture.

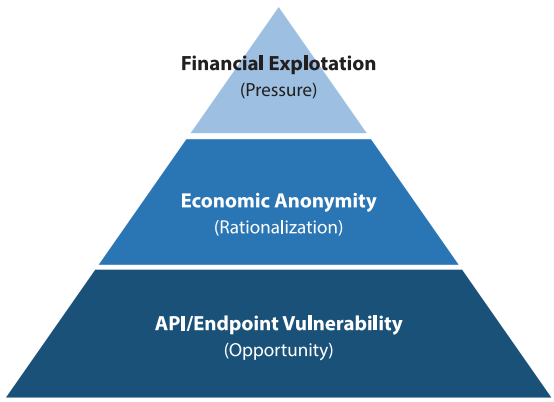
**Table 5: Mapping Forensic Interventions to DPI Threat Vectors**

| Identified Threat Vector | Traditional Audit Shortfall | Required Forensic Accounting Intervention |
|---|---|---|
| Synthetic Identities (ULI) | Relies on static and historical KYC documents. | Implementation of behavioural biometrics and cross-referencing disparate digital footprints. |
| Micro-Structuring (UPI) | Sample-based transaction testing misses low-value networks. | Automated Link Analysis and Graph Theory to map illicit fund flow networks. |
| Wallet Compromise (CBDC) | Cannot verify the legitimacy of cryptographic signatures post-facto. | Blockchain forensic tracing algorithms are embedded at the institutional node level. |

Source: Compiled by Author

Table 5 presents the theoretical data requirements for setting up Continuous Control Monitoring (CCM) systems. In developing these rules, there are several metrics defined: transaction velocity (requests per minute) vs value, so that the machine-learning algorithms can distinguish legitimate retail transactions from coordinated financial cyber crime in order to set up quantitative rules for these two types of transactions, which make up the logic for automated forensic intercepts at a financial institution's switch.

**Figure 5: The Digital Payment Fraud Triangle**




Source: Compiled by Author

Figure 5 provides a conceptual redesign of Cressey's well-known Fraud Triangle geared toward the architecture of Digital Public Infrastructure. The typical human-driven behaviour in traditional fraud can now be replaced by systemic flaws in technology (i.e. API/endpoint vulnerabilities, economic anonymity and financial exploitation). As a result of these changes, the diagram illustrates a different approach to fraud prevention. In the fast-paced digital world, forensic accounting should focus on identifying structural IT vulnerabilities and algorithmic anomalies proactively rather than on assessing the historical intent of the individuals involved.

**Discussion: Towards a Forensic-by-Design Framework**

The evidence-based analysis of aggregated transaction volume historical data, together with historical data on system downtimes, leads to one inescapable conclusion concerning the state of transaction processing systems: the infrastructure itself possesses high levels of robustness, but the proportionate nature of its resilience is structurally asymmetric. As evidenced by significant downtime at Grameen banks and designated payments banks due to substandard IT infrastructure, these locations are precisely the nodes cybercriminals exploit by injecting fraudulent requests or establishing mule accounts at lower-performing locations.

With the establishment and automation of the credit sanctioning process via API connections to land registry and GST portals, the time for a human underwriter to identify an anomaly is eliminated, leaving predictive modelling as the transition point for forensic accounting.

***Proposed Solutions and Regulatory Interventions***

To safeguard the future of India's DPI, the regulatory interventions will be required.

**Table 6: Proposed Forensic Compliance Framework for DPI Ecosystems**

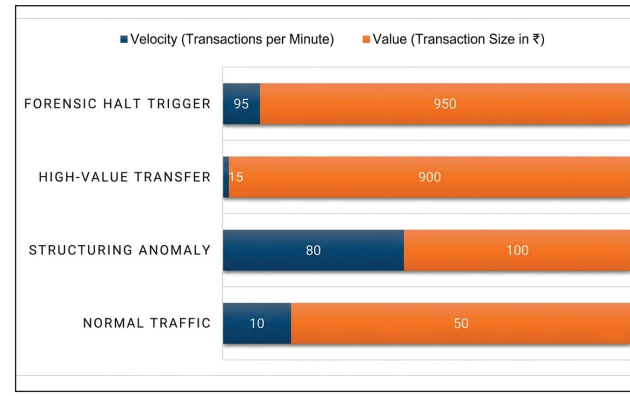
| Initiative | Target System | Implementation Strategy | Responsible Entity |
|---|---|---|---|
| Continuous Forensic Auditing (CFA) | UPI Switch | Mandate real-time anomaly detection APIs alongside payment gateways. | NPCI and Partner Banks |
| Identity Traceability Protocol | ULI | Embed forensic data validation algorithms before credit generation. | Credit Information Companies |
| Ledger Endpoint Security Validation | CBDC | Annual mandatory digital forensic audits of institutional wallet infrastructure. | RBI and Scheduled Banks |

Source: Compiled by Author

Table 6 shows India's Digital Public Infrastructure (DPI) transitioning from a reactive to a proactive approach through a "Forensic-by-Design" architecture. This framework identifies forensic initiatives and their respective target systems (i.e. Unified Payments Interface (UPI), Unified Lending Interface (ULI) and Central Bank Digital Currency (CBDC)) and converts the theoretical concept of risk mitigation into practical regulatory mandates. For example, a Continuous Forensic Audit (CFA) mandate associated with the UPI switch requires that both the National Payments Corporation of India (NPCI) and participating banks embed algorithmic anomaly-detection APIs into their payment gateways to nullify micro-structuring at the point of initiation effectively.

Another example is found in the context of the ULI, where the requirement for the "Identity Traceability Protocol" demonstrates that Credit Information Companies are tasked with validating behavioural biometrics before approving automated credits to their member institutions. With respect to the CBDC, this framework moves the audit focus away from the immutable central ledger and toward performing "Endpoint Security Validation" at the institutional wallet level. Ultimately, this table format serves as a prescriptive guide for regulators that highlights that developing a resilient system requires custom, hard-coded forensic interventions differentiated based upon the particular structural mechanics associated with each respective digital payment type.

**Figure 6: Forensic Alert Threshold Configuration**




Source: Compiled by Author

Figure 6 plots the normative financial behaviour that visually separates from forensic anomalies. The spatial clustering vividly demonstrates how continuous auditing operates in real-time. Transactions in the high-velocity and high-value quadrant immediately trigger an automated "Forensic Halt," disrupting the flow of illicit capital before settlement. This visualisation exemplifies the goal of "Forensic-by-Design", replacing post-facto human investigation with deterministic, algorithmic prevention.

**The Role of Forensic Accounting in Mitigating Systemic Digital Risk**

As the DPI evolves from a payment rail (UPI) to a credit engine (ULI) and a sovereign ledger (CBDC), traditional post-facto auditing becomes functionally obsolete. Forensic accounting must transition from a reactive investigative tool into a proactive and embedded security architecture.

***Algorithmic Tracing in High-Velocity Networks (UPI)***

In the UPI environment, primary function of Forensic accounting is to identify cluster formations of anomalies in real time. Forensic accountants can map complex networks of mule accounts using techniques such as Graph Theory and Link Analysis. Forensic algorithms must determine the velocity of an incoming transfer from the receiving account to the downstream accounts that will subsequently receive a transfer from that account. Any accounts that exhibit immediate and/or high-volume dispersal of incoming funds will be flagged for freezing; this action disrupts the cycle of money laundering before funds are withdrawn from the financial services industry.

***Behavioural Biometrics and Synthetic Identity Detection (ULI)***

The Unified Lending Interface presents challenges regarding automated sanctions on credit based on aggregated API data. Thus, forensic accountants will shift their focus from determining the integrity of the data stream to validating it before generating credit for the client. Therefore, forensic professionals will create systems to analyse behavioural biometrics, including typing cadence, device fingerprinting and geolocation anomalies, to detect "Synthetic Identities." Therefore, if a ULI credit application contains legitimate Goods and Services Act (GST) data but originates from a device or user with a history of credential stuffing, the forensic process will prevent automated approval of the credit application and require the forensic application and the credit request to undergo human-based investigative review.

***Cryptographic Ledger Auditing (CBDC)***

The rollout of the digital Rupee (e₹) means forensic accountants will need to find a way to bridge the gap between the auditing of fiat money and forensic analysis of blockchain. Although the Central Bank uses an immutable distributed ledger (blockchain) to record transactions, retail wallets that interact with the network are susceptible to key theft and malware. Forensic accountants will utilise both "Smart Contract Audits" and ongoing monitoring of the flow of digital tokens to detect when wallets have been compromised when using programmable money, preventing those funds from being irretrievably sent to dark web mixing services.

**Practical Implementation for Banking and Finance Professionals**

Banking professionals must operationalize theoretical forensic frameworks to safeguard institutional integrity. The following practical implementations are essential:

***Transitioning to Continuous Control Monitoring (CCM)***

The dependence on periodically conducted, sampling-derived internal audits must be eliminated for finance professionals. Moving to Continuous Control Monitoring (CCM) requires embedding forensic data analytics directly into the Core Banking System (CBS) of a financial institution, so that all digital transactions can be tested against a complete population using a predetermined forensic rule set. As soon as an anomalous transaction pattern is detected, such as an unexpected increase in transaction velocity from a dormant account, an automated alert will be triggered in milliseconds.

***Establishing Digital Forensic Incident Response (DFIR) Units***

Banks must restructure their risk management departments to include specialized Digital Forensic Incident Response (DFIR) units. These cross-functional teams, comprising forensic accountants, cyber security experts and legal professionals, must

be able to immediately quarantine compromised API endpoints, execute volatile memory captures on affected servers and preserve digital evidence in accordance with the Information Technology Act, 2000, ensuring admissibility in a court of law.

***Enhanced Inter-Institutional Threat Intelligence Sharing***

Given the interoperability of DPI, a cyber-attack on one institution can threaten the entire network. Finance professionals must actively participate in secure and anonymised threat intelligence-sharing platforms. By pooling forensic data on new phishing vectors, synthetic identity signatures and compromised mule account lists, the banking ecosystem can establish a collective and proactive defence mechanism.

**Challenges and Future Directions**

While the integration of forensic accounting into digital payments offers a robust defence, several systemic challenges remain:

***Interoperability Hurdles***

An inconsistent set of regulations and resources have created a large challenge. Banks receive detailed, tight guidance from the RBI on Cyber Security. In comparison, many smaller co-operative banks lack the resources to invest in the advanced forensic tools necessary to maintain a strong Cyber Security program. Because of this regulatory arbitrage, these smaller institutions represent a weak link in the overall network of interconnected Digital Payment Infrastructure (DPI) systems. In the future, it would be beneficial that all institutions, including the co-operative banks, implement a minimum "Forensic-by-Design" Infrastructure Standard for connecting to any UPI, ULI or Central Bank Digital Currency (CBDC) switch.

***The AI Arms Race in Financial Crime***

In an era where technological advancement has driven every aspect of life, the future of digital crime will be algorithmic. Cybercriminals are using Artificial Intelligence (AI) and more specifically Generative AI, to automate phishing campaigns, generate fraudulent KYC videos using deepfake technology and develop virally self-mutating malware that can circumvent static firewall rules. Consequently, forensic accounting needs to move toward predictive forensics and use adversarial machine learning to anticipate an AI-based cyber-attack and neutralise it before it breaches the bank's perimeter.

***Privacy Paradox in CBDC Implementation***

The rollout of retail CBDCs faces the challenge of balancing forensic traceability with individual privacy rights. Designing cryptographic protocols that allow the Law Enforcement Agencies (LEAs) to trace illicit funds without establishing a surveillance state remains a critical area for future academic and technical research.

**Conclusion**

The introduction of UPI, ULI and CBDC into India's financial transactions has ushered in a remarkable era of digitisation. Despite this success, findings from this study on transaction velocity, ecosystem growth and downtime due to infrastructure constraints reveal an alarming truth: Financial digitisation has created an ever-expanding cyber-attack surface. Traditional methods of auditing financial records—mainly reconciling previously recorded data—will not provide adequate protection over nearly instantaneous and real-time public infrastructure. The continued viability and integrity of these public infrastructures depend on the prompt and universal implementation of forensic accounting practices to monitor all abnormal transactions and shift from traditional auditing to continuous, automated forensic monitoring to protect India's digital financial architecture from the scale of modern-day organised cyber crime.

**Policy and Regulatory Recommendations**

To ensure that India's fast-growing Digital Public Infrastructure has robust financial support, regulatory authorities and industry groups should require that all participating financial institutions adopt a "Forensic-by-Design" architecture. The coordinated efforts on Regulatory Framework Enhancement,

Capacity Building in Forensic Accounting, Real-time Monitoring and Reporting Mechanisms, Incident Reporting Protocols and Collaborative Risk Assessment initiatives are required. This means changing the way regulations operate, from focusing on whether requirements were met after an event to Continuous Control Monitoring (CCM), which includes hard-coding anomaly-detection APIs and behavioural biometrics into switches for UPI and ULI transactions to eliminate synthetic identity fraud and micro-structuring proactively. The systemic infrastructure downtime as a major security incident can be considered, so that mandatory independent digital forensic audits are performed for any high-downtime nodes to ensure that typical outages are not concealing a concurrent cyber intrusion or data breach. Ultimately, implementing these in-house forensic measures and enabling advanced certification programs for bank employees will help transform the ecosystem from merely reactive to an evidence-based, proactive defence, thereby, supporting the continual resilience of the sovereign entity's digital payment and credit networks.

**References**


Brühl, V. (2026), "The potential impact of a Central Bank Digital Currency (CBDC) on the banking sector: The case of a digital euro", *Eurasian Economic Review*. https://doi.org/10.1007/s40822-025-00359-2.

Chidipothu, V. K., Vengaiah, C., Santosh, K., Abdurasul, B., G, S. and Manochitra, S. (2026), "Real-time synthetic identity fraud detection using recurrent neural networks for sequential data analysis", 2026 Sixth International Conference on Advances in Electrical, Computing, *Communications and Sustainable Technologies (ICAECT)*, pp. 1–5. https://doi.org/10.1109/icaect68478.2026.11426024.

Chinkhando Banda, M. R., Thakkar, H., Datta, S., Barot, H. and Jadav, J. (2025), "The impact of forensic accounting: A tool for fraud detection and prevention in the public sector in Malawi", *International Research Journal of Multidisciplinary Scope*, Vol 06 No 04, pp. 1017–1035. https://doi.org/10.47857/irjms.2025.v06i04.06423.

Correia, J. C. (2026), "Alternative Digital Platforms and the Renewal of the Public Sphere: Decidim and the Democratic Governance of Participatory Infrastructures", *Social Sciences*, Vol. 15 No 3, 166. https://doi.org/10.3390/socsci15030166.

Dattatreya Murthy, S. (2026), "Identity theft detection at data ingestion using AI: An explainable anomaly detection approach", *American Journal of Software Engineering*, Vol. 9 No 1, pp. 1–9. https://doi.org/10.12691/ajse-9-1-1.

Desai, R. and Bhatt, K. (2025), "Digital Finance and personality traits interplay in determining central bank digital currency adoption: Extending the Technology Acceptance Perspective", *International Journal of Bank Marketing*, Vol. 44 No 3, pp. 571–594. https://doi.org/10.1108/ijbm-02-2025-0154.

Dimitropoulos, G., & Reading, M. (2025), "Forensic accounting as an investigative tool: Insights from the FTX and Qatargate", *Journal of Economic Criminology*, Article 100132, https://doi.org/10.1016/j.jeconc.2025.100132.

Ghosh, K. and Das, P. K. (2026), "Understanding Central Bank digital currency adoption: A bibliometric and AI-driven analysis", *Digital Policy, Regulation and Governance*, pp. 1–16, https://doi.org/10.1108/dprg-11-2025-0439.

Hoti, A., Qehaja, D., Buçaj, E. and Qehaja-Keka, V. (2025), "Ai-enhanced auditing and regulatory compliance: Balancing Innovation with accountability", *Sustainable Finance*, pp. 423–445, https://doi.org/10.1007/978-3-032-01677-5_19.

Indian Computer Emergency Response Team (CERT-In), (2024), Annual report 2024. Ministry of Electronics and Information Technology, Government of India, https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2025-0001.pdf.

National Payments Corporation of India (n.d.), UPI product statistics, https://www.npci.org.in/product/upi/product-statistics.

Jaison P A., Jayan, M. and JS, S. (2026), "From connectivity to crisis: A Socio Technological Study of Internet Failures and UPI payment disruptions",

*SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.6355458.

Rabha, M. P. and Chourasia, B. (2025), "UPI And Green Economy: A Study On Reducing Carbon Footprints Through Digital Payments", *Journal of Applied Bioanalysis*, Vol. 11 No 15, pp. 684–691, https://doi.org/10.53555/jab.v11si15.2200.

Sampathkumar, V., Kotha, R. and Ramaraj, D. K. (2026), "Reinforcing digital banking onboarding with generative AI Fraud Detection", 2026 IEEE 16th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0133–0141, https://doi.org/10.1109/ccwc67433.2026.11393774.

Sateesh Kumar, T. K., Thomas, J., Thomas, L. and Menon, V. A. (2025), "Forecasting UPI transaction value in India", *Advances in Computational Intelligence and Robotics*, pp. 33–56, https://doi.org/10.4018/979-8-3373-5747-8.ch002.

Thakkar, H., Datta, S. and Devi, A. (2025), "Border Security and Economic Growth: A Bibliometric Assessment", *Obrana a Strategie (Defence & Strategy)*, Vil. 25 No 2, 245, https://doi.org/10.3849/1802-7199.25.2025.02.245-265.

Thakkar, H., Datta, S., Bhadra, P., Barot, H. and Jadav, J. (2025), "Artificial Intelligence and machine learning in fraud detection: A comprehensive bibliometric mapping of research trends and directions", *Annals of Library and Information Studies*, Vol. 72 No 2, https://doi.org/10.56042/alis.v72i2.14752.

Thakkar, H., Datta, S., Bhadra, P., Barot, H., Purohit, M. and Dabhade, S. (2024), "A bibliometric analysis of forensic accounting research: Unveiling its impact on tax fraud detection in SAARC countries", *Journal of Informatics Education and Research*, https://doi.org/10.52783/jier.v4i2.1031.

Thakkar, H., Datta, S., Bhadra, P., Dabhade, S. B., Barot, H. and Junare, S. O. (2024), "Mapping the knowledge landscape of money laundering for terrorism financing: A Bibliometric analysis", *Journal of Risk and Financial Management*, Vol. 17 No 10, 428, https://doi.org/10.3390/jrfm17100428.

Thakkar, H., Fanuel, G. C., Datta, S., Bhadra, P. and Dabhade, S. B. (2025), "Optimizing Internal Audit Practices for combatting occupational fraud: A Study of Data Analytic Tool Integration in Zimbabwean listed companies", *International Research Journal of Multidisciplinary Scope*, Vol. 06 No 01, pp. 22–36, https://doi.org/10.47857/irjms.2025.v06i01.02164.

Wang, M., Zhang, J. and Xia, X. (2026), "Building Digital Bridges: Spillover Effects of Public Infrastructure Investment", *Eurasian Business Review*, https://doi.org/10.1007/s40821-025-00338-2.