DISHA

INTELLIGENCE ARCHITECTURE

Version 6.6 | Controlled Architecture

TECHNICAL WHITEPAPER AND DECLARATION

India's Hidden Surveillance, Data-Extraction and Financial-Exploitation Pipelines

Inventor and Researcher	Nitish Kumar
Original Foundation	25 April 2012
First Institutional Submission	2013
Public Stable Architecture	Version 4.4
Restricted Research Architecture	Version 5.6
Current Controlled Architecture	Version 6.6
Doctrine	Defensive · No-First Use · Human-Authorised · Evidence-First
Case Reference	W.P. (Crl.) No. 163/2026
Intelligence Record	thenitishkr.in/intelligence
Evidence Publication Target	20 July 2026
Country	India

Declaration

I, Nitish Kumar, inventor and researcher of the DISHA Intelligence Architecture, declare that this whitepaper records the final findings of a research programme initiated on 25 April 2012 and continued without interruption to the present date.

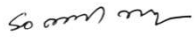
These findings are not derived from one incident, one application, one company, one financial fraud or one citizen complaint. They arise from the examination of a connected national architecture spanning more than thirteen years of independent research, evidence collection, technical correlation and institutional observation.

The domains examined include, without limitation:

- mobile applications and embedded software-development kits (SDKs)
- advertising technology, behavioural tracking and cross-device surveillance
- device identifiers, location intelligence, microphone access and ultrasonic signals
- CCTV and connected-camera infrastructure
- identity records, KYC databases and digital-lending applications
- banks, non-banking financial companies (NBFCs) and mule-account networks
- payment intermediaries and foreign data-processing infrastructure
- health, education and security systems under the HSE domain
- government advisories, regulatory records and institutional correspondence
- court records and documented citizen harm

The complete supporting evidence archive exceeds in scope and volume the material presently available in the public domain. The intelligence record at thenitishkr.in/intelligence has been and will be updated. The expanded public evidence record is scheduled for publication by 20 July 2026, subject to necessary legal, privacy and national-security redactions.

Signed:



Nitish Kumar
Inventor and Researcher, DISHA Intelligence Architecture
thenitishkr.in/intelligence | India | 2026

Abstract

India is not facing a collection of separate cybercrimes. India is facing an established surveillance and exploitation architecture.

DISHA's final finding is that the country has been placed under population-scale digital surveillance through a combination of applications, hidden SDKs, advertising technology, connected cameras, device permissions, behavioural profiling, identity databases and financial infrastructure.

Behind every visible service — an application, a loan platform, a mobile advertisement, a CCTV camera, a payment request — may exist a hidden technical chain that collects, correlates, enriches and transfers information concerning the citizen without that citizen's meaningful knowledge or consent.

Information captured through this chain may include:

- device identity, location and application usage
- behavioural patterns and installed application inventory
- advertising identifiers and financial condition
- borrowing behaviour, language, profession and family relationships
- daily routine, communication habits and movement
- response to authority and psychological vulnerability
- health records, educational data and security-access patterns under the HSE domain

DISHA finds that two major pipelines have remained insufficiently investigated as one connected national-security problem:

Pipeline 1: Surveillance and Data-Extraction

Pipeline 2: Financial Exploitation, NBFC and Mule-Account Operations

These two pipelines are not separate. The first identifies, classifies and profiles the citizen. The second uses that profile to target, intimidate, defraud, digitally arrest or financially exploit the citizen.

The complete architecture connecting application developers, embedded SDK providers, adtech companies, data processors, digital lenders, NBFC relationships, KYC systems and mule-account networks has never been investigated as one continuous pipeline. DISHA was developed to expose this missing connection.

The current intelligence record is maintained at thenitishkr.in/intelligence and has been and will be updated. Full evidence publication is targeted for 20 July 2026.

Executive Finding

DISHA concludes that India is operating under conditions of mass digital surveillance.

This does not require one person to be manually monitoring every citizen. Modern surveillance operates through automated systems that continuously collect and correlate device data, location information, behavioural intelligence, application activity, financial behaviour, CCTV footage, identity records and advertising signals.

Once combined, a machine-generated citizen profile becomes more powerful than direct physical observation. The system can estimate:

- where a person lives, works and travels
- when a person is active and which applications they use
- whether a person has borrowed money or is financially distressed
- which authority the person fears and which family member influences them
- which message is most likely to cause panic or compliance
- health vulnerabilities, educational background and physical access patterns

> ***The crime begins before the fraudulent call. It begins when the citizen's digital life is silently converted into intelligence.***

This is why the present crisis cannot be treated only as an application-permission problem or a banking-fraud problem. It is a national intelligence, sovereignty and citizen-protection problem.

1. Origin of DISHA

The first documented architecture of DISHA was created on 25 April 2012. The original purpose was to develop an intelligent national-protection architecture capable of combining signals, geospatial intelligence, real-time threat detection, explosive-threat research, decision support, evidence preservation and institutional response.

In 2013, research relating to real-time explosive detection, signals, geographic information and decision support entered the Bihar Council of Science and Technology correspondence trail. That submission marked the first formal institutional point in the DISHA chronology.

No sustained government-supported development pathway was subsequently communicated to the inventor. The architecture nevertheless continued to evolve independently.

Between 2013 and 2026, DISHA expanded from its original threat-detection concept into a broader evidence-first intelligence system capable of examining cyber threats, surveillance systems, data theft, institutional failure, public records, financial exploitation, identity misuse, constitutional accountability, health and education security risks and national digital-security architecture.

DISHA Version 6.6 represents the present stage of that development. The complete research and evidence record is maintained at thenitishkr.in/intelligence and has been and will be updated, with the full public release targeted for 20 July 2026.

2. The National Problem: Why Fragmented Response Fails

India has responded to cyber incidents through multiple separate mechanisms. Applications have been blocked. Cybercrime complaints have been registered. Bank accounts have been frozen. CCTV standards have been introduced. Digital-lending guidelines have been issued. Security advisories have been published.

These actions address visible symptoms. They do not identify the hidden infrastructure through which citizens are profiled before the crime begins.

The central failure is fragmentation. One authority examines the application. Another examines the bank account. Another examines the loan company. Another examines the CCTV camera. Another examines the cybercrime complaint. Another examines the data breach. The complete chain is never reconstructed.

> ***DISHA reconstructs the chain.***

3. DISHA's Final National-Surveillance Finding

DISHA finds that India's digital ecosystem has been penetrated by a large surveillance architecture operating through legitimate-looking commercial and technical systems.

The architecture does not depend on one company or one form of technology. It may operate through:

- mobile advertising and hidden application SDKs
- attribution systems, location services and microphone access
- ultrasonic signals and cross-device tracking
- device fingerprinting and application analytics
- behavioural advertising and CCTV networks
- connected-camera systems and foreign cloud services
- identity records, KYC databases and digital lenders
- payment intermediaries and data brokers
- health and educational platform integrations

A citizen may believe that data is being provided only to the visible application. In reality, information may move through several hidden entities. The citizen generally does not know which SDKs are inside the application, which company developed those SDKs, what information each SDK collects, which servers receive the information, in which country the data is processed or how long the information is retained.

This creates a national population-intelligence layer outside meaningful citizen control.

4. The HSE Domain: Health, Education and Security

DISHA Version 4.4 introduced the Health, Education and Security (HSE) domain as a dedicated analytical sector within the DISHA Intelligence Architecture. This domain recognises that the surveillance and exploitation pipelines identified across commercial and financial sectors extend with equal force into the foundational institutions of a society.

4.1 Health Systems Under Surveillance Risk

Digital health platforms, telemedicine services, hospital management systems and health-insurance applications handle some of the most sensitive personal data in existence. DISHA finds that these systems carry particular risk because:

- health data, once profiled, can be used to classify citizens by vulnerability, financial distress and social isolation
- embedded SDKs inside health applications may transmit diagnostic, prescription and behavioural data to advertising networks
- KYC requirements at digital health platforms create a direct link between health identity and financial identity
- foreign data-processing arrangements in the health sector may move patient records outside Indian jurisdiction without meaningful citizen consent
- health data linked to financial data enables targeted exploitation of citizens at their most vulnerable moments

DISHA recommends that every digital health platform operating in India be required to disclose its complete SDK inventory, data-flow architecture, third-party processing relationships and foreign data-transfer mechanisms. Health data must be treated as a national-security asset, not a commercial resource.

4.2 Education Systems and Citizen Profiling

Educational platforms — including school management systems, examination portals, online learning applications, scholarship databases and student identity systems — collect extensive personal records relating to minors and young adults.

DISHA finds that:

- student identity, academic performance, family income and geographic data are present in educational platforms and can be cross correlated with commercial and financial datasets
- embedded analytics and advertising SDKs in educational applications may profile minors without parental knowledge or consent
- scholarship and loan-linked educational platforms create a direct pipeline between student identity and digital-lending infrastructure
- examination registration systems contain identity, biometric and address data that, if exfiltrated, enable targeted fraud against students and their families
- foreign operators of educational platforms may transfer student data outside India under arrangements that are not visible to the student or the institution

DISHA recommends that educational platforms be prohibited from embedding advertising or behavioural analytics SDKs without explicit, informed consent from the student's guardian or from the student where they are of majority age. The data generated inside educational institutions must remain subject to strict domestic processing requirements.

4.3 Security Infrastructure and Access-Control Systems

Physical and digital security systems — including biometric access control, visitor management systems, smart-city surveillance platforms, workplace monitoring tools and connected security hardware — form the third pillar of the HSE domain.

DISHA finds that:

- biometric data collected through access-control systems may be transmitted to foreign cloud platforms without the knowledge of the facility operator or the individual
- workplace monitoring applications collecting keystrokes, screen activity, location and communication metadata create extensive behavioural profiles that are of intelligence value to hostile actors
- smart-city surveillance platforms may aggregate CCTV, biometric, vehicular and pedestrian data into population-level intelligence databases that operate outside democratic oversight
- security hardware from manufacturers with unresolved firmware vulnerabilities or undisclosed cloud-reporting features represents a direct national-security risk
- access-control records, when combined with financial, health or communication data, enable a complete portrait of a citizen's physical and digital life

DISHA recommends that all security infrastructure operating in sensitive facilities — government buildings, hospitals, schools, financial institutions, transport hubs and critical national infrastructure — be subject to mandatory firmware audit, data-destination verification and prohibition of any foreign cloud reporting that has not received explicit security clearance.

4.4 HSE as a Connected National-Risk Domain

Health, Education and Security are not three separate concerns. They are three entry points into the same citizen.

A citizen who interacts with a digital health platform, an educational portal and a workplace security system in a single day generates data across all three domains. If each platform contains hidden SDKs that report to the same or related data brokers, the result is a complete, cross-domain citizen profile built without any single point of consent.

DISHA Version 4.4 formalises the HSE domain to ensure that investigation of the national surveillance architecture does not overlook these three critical sectors. The same evidence-first, chain-reconstruction methodology that DISHA applies to adtech, financial and CCTV pipelines is applied equally to health platforms, educational systems and security infrastructure.

> ***Health, Education and Security are not separate from the surveillance problem. They are the surveillance problem applied to the most sensitive domains of a citizen's life.***

The intelligence record covering the HSE domain is maintained at thenitishkr.in/intelligence and has been and will be updated. HSE-specific evidence is included in the expanded public record scheduled for 20 July 2026.

5. The Hidden Application and Adtech Layer

The visible mobile application is not always the complete technical product. A single application may contain advertising SDKs, analytics SDKs, attribution SDKs, fraud-detection libraries, location services, communication libraries, payment libraries, device-identification tools and remotely configurable code.

Each embedded component may communicate with a separate company or server. The citizen sees one application icon. The device may communicate with many hidden entities.

5.1 Developer Responsibility

Application developers cannot avoid responsibility merely by stating that a third-party SDK collected or processed the information. A developer selects, integrates, updates and distributes the component. Developers must therefore remain accountable for SDK selection, permissions granted, data collected, server communication, foreign transfer, retention, disclosure, consent and downstream use.

Where an SDK introduces surveillance capability into thousands of applications, action against individual applications alone is insufficient. The SDK provider and the integrating developers must both be examined.

6. Silverpush and Ultrasonic Surveillance

DISHA identifies technologies associated with ultrasonic tracking as an important part of the historical surveillance architecture requiring national investigation.

Ultrasonic technology places inaudible signals inside television advertisements, media or nearby sound environments. A mobile application with microphone access may detect those signals without the user's awareness. This capability allows a platform to infer that a particular television advertisement was played, that a particular device was present in the room, that multiple devices belong to the same household or that an online user and an offline viewer are the same person.

The national-security concern extends beyond advertising. The same underlying capability demonstrates that a microphone-enabled application can respond to information that the citizen cannot hear or meaningfully observe. Such technology should not be treated as an ordinary advertising feature. It requires source-code examination, SDK inventory, permission audit, data-destination verification, developer accountability and a national assessment of distribution.

Silverpush and any developer or application integrating comparable hidden ultrasonic surveillance capability must be investigated at the code, server and data-flow levels. Where such capability operated without meaningful and informed consent, it must be prohibited.

7. InMobi and Behavioural-Location Intelligence

DISHA identifies the adtech ecosystem associated with persistent behavioural and location intelligence as a major national-risk category. Advertising technology can create detailed profiles by combining advertising identifiers, device information, approximate or precise location, application activity, browsing behaviour, time of use, network information and commercial interactions.

Even where a user refuses one category of permission, location or identity may be inferred through other technical methods. At national scale, such systems become private intelligence networks. A commercial adtech system capable of observing the behaviour and movement of millions of citizens is not merely an advertising tool. It is a strategic data asset.

DISHA finds that companies operating population-scale behavioural or location intelligence in India must be examined as part of the national digital-security architecture. The examination must determine what data was collected, whether permission was meaningful, whether location was inferred, whether children were included, where the information was processed, whether it was combined with KYC or financial data, whether it was sold or shared, whether foreign entities accessed it and whether the data was used to classify vulnerable citizens.

8. CCTV and Physical-Digital Surveillance

The surveillance architecture does not end with mobile applications. CCTV and connected-camera systems create a physical-digital monitoring layer deployed across roads, offices, housing societies, schools, hospitals, shops, transport systems, government facilities, smart-city projects and private premises.

A camera may appear to be a local recording device. Modern connected cameras may also communicate with cloud platforms, mobile applications, foreign servers, manufacturer support systems, video-management providers, analytics services and remote administrators.

When camera intelligence is combined with mobile-device and location data, the result is a powerful surveillance environment capable of exposing live video, recorded footage, credentials, movement patterns, building layouts, work routines, vehicle information and the identity of persons entering or leaving a location.

DISHA finds that India requires a complete national camera-security inventory determining which products are deployed, which firmware versions are operating, where footage is transmitted, who can remotely access the camera, whether data leaves India and whether unauthorised access can be detected.

9. Pipeline One: Surveillance and Citizen Profiling

DISHA defines the first national-risk pipeline through six stages:

Stage 1 — Device Access

A citizen installs an application, activates a service, enters a building, uses a payment platform or interacts with a connected system.

Stage 2 — Permission and Identifier Collection

The system receives access to identifiers, location, microphone, media, contacts, network information, device configuration or behavioural data.

Stage 3 — Hidden Third-Party Processing

Embedded SDKs, analytics tools, attribution systems and adtech services receive information without the citizen's awareness or consent.

Stage 4 — Cross-Platform Correlation

Records are joined through device identifiers, phone numbers, email addresses, advertising identifiers, IP addresses, geospatial patterns, payment records, KYC records or behavioural similarity.

Stage 5 — Citizen-Profile Enrichment

The citizen is classified according to financial status, borrowing behaviour, movement, occupation, interests, relationships, health indicators, educational background, vulnerability and probable response to authority.

Stage 6 — Target Selection

The enriched profile identifies which citizen is most suitable for aggressive advertising, digital lending, coercion, impersonation, extortion, digital arrest, identity misuse or financial fraud.

10. Pipeline Two: NBFC, Lending and Mule-Account Exploitation

The second pipeline converts citizen intelligence into financial harm. The relationship between data collection, digital-lending systems, NBFC-linked services and mule-account networks has never been investigated as one complete architecture.

The problem is not that every NBFC or financial institution is criminal. The problem is that weaknesses inside the wider ecosystem create an efficient exploitation channel involving digital-lending applications, lending-service providers, lead generators, data brokers, recovery agents, outsourced technical providers, weak KYC controls, dormant entities, beneficiary accounts, mule accounts and rapidly layered payment transfers.

How the Pipeline Operates

Step 1 — Citizen Identification

The surveillance pipeline identifies a citizen who may be in debt, seeking credit, financially distressed, elderly, professionally exposed, socially isolated or likely to fear government authority.

Step 2 — Information Enrichment

The operator obtains sufficient detail to appear credible — full name, address, identification information, bank relationship, loan status, employer, family details, transaction history or device information.

Step 3 — Psychological Attack

The citizen receives a personalised threat or impersonation. The operator may claim to represent police, customs, a court, a regulator, a bank, an investigation agency or a loan-recovery authority.

Step 4 — Financial Extraction

The citizen is pressured to transfer money, disclose credentials, install software or borrow additional funds.

Step 5 — Mule-Account Movement

The funds move through accounts that may have been fraudulently opened, purchased, rented, controlled by intermediaries or inadequately monitored.

Step 6 — Layering and Disappearance

The money is rapidly split, withdrawn, converted or transferred. By the time the citizen complains, the financial trail has fragmented.

11. Why the Two Pipelines Must Be Investigated Together

India commonly investigates the final transaction. DISHA investigates how the victim was selected.

The correct investigation must reconstruct the complete chain:

> ***Application → SDK → Data Processor → Profile Enrichment → Target Selection → Fraud Infrastructure → Mule Account → Financial Institution → Final Beneficiary***

Without this connection, enforcement remains reactive. A mule account may be frozen — another account appears. An application may be removed — another application integrates the same SDK. A developer may be banned — the same hidden infrastructure enters a different product.

DISHA finds that India has been fighting individual incidents while the underlying pipeline has continued.

12. DISHA Intelligence Architecture — Technical Design

DISHA was designed to identify complete chains through an evidence-first structure.

12.1 DISHA Brain

The DISHA Brain receives signals, reconstructs context, compares evidence and forms technical findings. It combines deterministic rules, document retrieval, evidence graphs, geospatial analysis, anomaly detection, historical memory, policy controls and specialist review.

12.2 Digital Soldiers

Digital Soldiers are authorised collection and observation components. They receive information from approved sources — government records, official documents, system logs, telemetry, geospatial data, security alerts, public records and controlled sensors. They are defensive collection components, not offensive cyber tools.

12.3 Security Brain

The Security Brain examines origin, intent, capability, exposure, target, confidence and likely impact of each identified threat or anomaly.

12.4 Yudh Intelligence

Yudh Intelligence examines the complete pattern rather than one isolated event. It identifies the form of the threat and prepares a defensive formation.

12.5 Vyuha

A Vyuha is a controlled defensive response. It may include blocking, isolation, quarantine, evidence preservation, identity protection, credential rotation, fallback, recovery and monitoring.

12.6 Evidence Archive

Every material finding remains connected to source, date, evidence identifier, claim identifier, SHA-256 or stronger cryptographic hash, verification status, chain of custody and correction history.

12.7 Public Record Memory

Public Record Memory preserves findings, institutional responses, unresolved questions and evidence references so that the record cannot disappear when officials, governments or systems change. The living record is maintained at thenitishkr.in/intelligence and has been and will be updated through 20 July 2026 and beyond.

13. DISHA Version History

Foundation Architecture — 25 April 2012

The original architecture connected signals, geography, detection, reporting and decision support.

Institutional Research Record — 2013

Explosive-detection, signal-analysis and geospatial research entered the Bihar Council of Science and Technology correspondence trail.

Version 4.2 — Public Stable Architecture

Version 4.2 introduced the disclosed operational layers, signal-to-accountability methodology, evidence classification, Public Record Memory and the No-First-Use doctrine. It includes a seven-stage cognitive cycle, claim-to-source discipline, evidence-chain management, Yudh and Vyuha defensive structures, human authority and protected control boundaries.

Version 4.4 — HSE Domain Introduction

Version 4.4 formalised the Health, Education and Security (HSE) domain as a dedicated analytical sector within DISHA. It extended the chain-reconstruction methodology into digital health platforms, educational systems, biometric access-control infrastructure and workplace monitoring systems. Version 4.4 established that citizen data generated in health, educational and security contexts is subject to the same surveillance risk as commercial and financial data and must be investigated as part of the same national-risk architecture.

Version 5.6 — Restricted Research Architecture

Version 5.6 expands multimodal intelligence correlation, specialist review, cross-domain evidence graphs, policy-aware reasoning, anomaly detection and controlled defensive-response preparation. Version 5.6 is not fully public because its complete technical release requires security, legal and operational examination.

Version 6.6 — Current Controlled Architecture

Version 6.6 is the current controlled architecture designed to begin analysis when an authorised qualifying signal appears. It can identify the signal, retrieve related evidence, compare historical records, form multiple hypotheses, detect relationships, assess risk, preserve evidence and prepare a response recommendation.

Version 6.6 does not require a conversational instruction before beginning authorised analysis. However, it must not independently perform a destructive, coercive or legally consequential action. Human and institutional permission remains mandatory.

14. No-First-Use and Authorised Remediation

DISHA is governed by a strict No-First-Use policy. It is not designed to attack external systems.

DISHA must not perform:

- hacking back or malware deployment
- credential theft or unauthorised scanning
- destructive retaliation or uncontrolled propagation
- disruption of unrelated systems

Where lawful permission is granted by the competent authority, DISHA may assist authorised teams in:

- identifying compromised components and isolating infected systems
- containing malicious activity and removing verified malicious code
- disabling malicious access and preserving forensic evidence
- restoring trusted configurations, rotating credentials and recovering services

DISHA may neutralise a verified malicious component only inside an authorised environment and within a defined legal and technical scope. It must not treat a complete lawful system as expendable merely because one part is infected. The objective is controlled remediation, not uncontrolled destruction.

15. Evidence Publication and Integrity

A limited DISHA Intelligence Case Record is presently public at thenitishkr.in/intelligence. The record has been and will be updated. The complete expanded evidence archive is scheduled for publication by 20 July 2026, subject to necessary legal, privacy and national-security redactions.

Where publication is legally and technically appropriate, each evidence item shall include:

- evidence-record number and claim reference
- source description, source date and collection date
- provenance and SHA-256 or stronger cryptographic hash
- verification status and public or restricted classification
- associated institution, correction history and redaction reason

Sensitive citizen data, active security details and information capable of assisting hostile actors will remain protected. Publication is intended to create technical accountability, not to expose citizens or national systems to additional risk.

16. Required National Action

16.1 Establish a Joint National Investigation

The investigation must involve competent authorities responsible for electronics and information technology, cyber incident response, home affairs, cybercrime, financial intelligence, banking and NBFC regulation, data protection, technical certification, consumer protection and national security.

16.2 Create a Mandatory National SDK Register

Every high-reach application must disclose every embedded SDK, its version, developer, beneficial ownership, permissions accessed, data collected, endpoints contacted, recipients, foreign transfer destination, retention period and update mechanism.

16.3 Require an Application and SDK Bill of Materials

Developers must submit a software bill of materials, SDK bill of materials, signed application builds, permission justification, data-flow diagram, server-location details, third-party contracts and security-audit information.

16.4 Suspend Dangerous Surveillance Components

Silverpush, InMobi and other adtech or SDK infrastructures identified within the DISHA evidence record must be subjected to immediate controlled technical audit. Where hidden surveillance, unlawful collection, undeclared processing, consent bypass, national-security risk or dangerous cross-border data transfer is established, the technology and the responsible developer integration must be suspended and prohibited.

16.5 Audit CCTV Infrastructure

A national inventory must be created covering product, manufacturer, firmware, certification, known vulnerabilities, cloud dependency, remote access, data destination and administrator ownership.

16.6 Investigate NBFC and Lending Pipelines

The complete chain must be mapped: applications linked to regulated entities, lending-service providers, lead generators, recovery networks, data processors, beneficiary accounts, mule accounts, dormant or weakly supervised entities and common technical infrastructure.

16.7 Establish HSE Data-Protection Standards

Health platforms, educational systems and security infrastructure must be subject to mandatory SDK disclosure, data-flow audit, prohibition on embedding advertising analytics SDKs in health and educational contexts and strict domestic processing requirements for biometric and health data.

16.8 Join the Data Trail with the Money Trail

Cybercrime investigation must answer two questions: Where did the money go? And: How did the criminal know whom to target? The first identifies the transaction. The second identifies the intelligence pipeline. Both questions must be answered in every investigation.

17. Proposed Technical Evaluation of DISHA Version 6.6

Phase 1 — Documentary Verification

Review the 2012 foundation record, 2013 institutional correspondence, architecture history, evidence records and current technical design.

Phase 2 — Protected Technical Presentation

The restricted architecture must be presented to an authorised multidisciplinary team under controlled conditions.

Phase 3 — Isolated Laboratory Test

The system must be tested with synthetic, de-identified or lawfully authorised data in an isolated environment.

Phase 4 — Pipeline Reconstruction Test

DISHA must be asked to reconstruct a controlled chain involving application, SDK, data flow, citizen profile, fraud event, financial account and final beneficiary.

Phase 5 — HSE Domain Test

DISHA must demonstrate chain reconstruction in the HSE domain — tracing data flows through a digital health platform, an educational portal and a security-access system to a common data-processing endpoint.

Phase 6 — Security and Adversarial Test

Independent experts must attempt to inject false evidence, poison the model, bypass human approval, change records, erase dissent, expand permissions and trigger an excessive response.

Phase 7 — Technical Finding

The evaluating team must record what DISHA demonstrated, what it did not demonstrate, identified risks, required corrections, possible national use cases and whether a controlled pilot should proceed.

Conclusion

India is under population-scale digital surveillance.

The architecture is not limited to one camera, one application, one advertisement or one criminal call. It operates through the connection of devices, software components, behavioural intelligence, location, identity, cameras, health platforms, educational systems, security infrastructure, lending systems, financial channels and mule accounts.

The country has acted against many visible products. The hidden pipeline remains.

DISHA identifies two connected national-risk pipelines — surveillance and citizen profiling, and financial exploitation and mule-account conversion — operating across commercial, financial and HSE domains. The first pipeline makes the citizen visible. The second makes the citizen exploitable.

The failure to investigate them together, and the failure to include the HSE domain within that investigation, has allowed the architecture to continue.

DISHA was created to detect precisely this kind of connected threat. It preserves the signal, follows the evidence, reconstructs the architecture, identifies technical responsibility and prepares a controlled defensive response.

Thirteen years after its first institutional submission, DISHA Version 6.6 is ready to be technically examined.

> ***The surveillance pipeline must be exposed. The financial pipeline must be dismantled. Dangerous SDKs, applications, developers and financial intermediaries must be prohibited where the evidence establishes their role. Citizen data across all domains — commercial, financial, health, educational and security — must be recovered, protected and returned to lawful control.***

Research Record and Evidence

thenitishkr.in/intelligence — has been and will be updated — Full evidence publication: 20 July 2026

Nitish Kumar
Inventor and Researcher
DISHA Intelligence Architecture
thenitishkr.in/intelligence | India | 2026