ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

The Cracks in the Foundation: UMANG and the Security of Digital Public Infrastructure

THE HINDU

15 July 2026 · POLITY · GS2 GS3

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Ujiyari Current Affairs
Daily Current Affairs for UPSC & State PCS · ujiyari.com
EDITORIAL ANALYSIS
15 July 2026

The Cracks in the Foundation: UMANG and the Security of Digital Public Infrastructure

The Hindu 15 July 2026 GS2 GS3

Source: ujiyari.com — researched, fact-checked & UPSC-mapped

THE LIFT LINE

Digital Public Infrastructure earns citizen trust by promising that convenience will not cost them their privacy, and a single unpatched flaw that exposes the Aadhaar and provident-fund details of millions is not a technical footnote but a breach of that founding promise.

WHY THIS EDITORIAL MATTERS FOR YOUR EXAM

In July 2026, security researchers Akshay C.S. and Viral Vaghela reported that the UMANG platform, the government's unified mobile gateway to hundreds of public services, carried vulnerabilities that could expose sensitive citizen data, including EPFO Universal Account Numbers, LPG booking details, and Aadhaar numbers stored in plaintext by linked services. The EPFO module alone logged over 400 million transactions in three months, so the exposure surface was vast. The researchers disclosed the flaws to MeitY and CERT-In, and while the ministry acknowledged the findings and said fixes were under way, the episode raises the central governance question of the digital state, whether India's Digital Public Infrastructure is secured by design or only patched after disclosure.

GS Paper 2: E-governance, government policies for the digital sector, and transparency and accountability. **GS Paper 3:** Cybersecurity, the role of security agencies, and challenges to internal security through communication networks.

For **Prelims**, hold the specifics: UMANG, the Unified Mobile Application for New-age Governance; the Digital Personal Data Protection Act, 2023 (https://ujiyari.com/legislation/dpdp-act-2023/), which imposes obligations on data fiduciaries, requires breach notification, and establishes the Data Protection Board; CERT-In, the national computer emergency response team under MeitY, with its incident-reporting directions; and

the concept of Digital Public Infrastructure spanning identity, payments, and data-sharing layers. For **Mains**, argue that as the state digitalises service delivery, cybersecurity ceases to be an IT concern and becomes a core duty of governance, since the state itself becomes the custodian of citizens' most sensitive data.

BACKGROUND AND CONTEXT

Digital Public Infrastructure is India's flagship governance model, a stack of shared digital systems, identity, payments, and data exchange, on which public and private services are built. Its promise is scale and inclusion. Its risk is concentration, because when hundreds of services sit on one gateway, a flaw in the foundation propagates across all of them.

The UMANG disclosure illustrates the concentration risk precisely. The researchers found that the weakness stemmed from the portal's underlying architecture rather than a single service, meaning the vulnerability (https://ujiyari.com/vocab/vulnerability/) was systemic. Storing identifiers such as Aadhaar numbers in plaintext, if confirmed, violates the elementary principle that sensitive data must be encrypted at rest. That such a lapse could persist in a heavily used government platform points to a gap between the ambition of the digital state and the discipline of securing it.

THE CORE ARGUMENT / ISSUE

Security by design, not by disclosure

A mature DPI treats security as a built-in property, with encryption, access controls, and audits designed in from the start. Relying on external researchers to surface flaws, and on patches after the fact, means citizens are protected only after they have already been exposed.

The DPDP Act and state accountability

The DPDP Act, 2023, makes any entity processing personal data a data fiduciary (https://ujiyari.com/terms/fiduciary/) bound to protect it and to notify breaches. Crucially, the state is not exempt from the duty of security. If a government platform stores identifiers unsafely, the Act's obligations, and the Data Protection Board's oversight, must apply with full force.

REQUIREMENT	WHAT GOOD DPI SECURITY DEMANDS	THE UMANG CONCERN
Data at rest	Strong encryption of identifiers	Sensitive data reportedly in plaintext
Architecture	Security designed into the core	Flaw stemmed from underlying architecture
Breach response	Prompt notification, CERT-In reporting	Fixes reportedly applied after disclosure
Accountability	Data-fiduciary duties on the state too	Enforcement clarity still evolving

Concentration and systemic risk

The very design that makes DPI powerful, one gateway to many services, magnifies the cost of a single failure. This demands a higher, not lower, security standard than a stand-alone application would require.

HOW TO THINK ABOUT THIS (ANALYTICAL FRAME)

Frame this as a trade-off between the efficiency of concentration and the fragility it creates. DPI delivers inclusion at scale precisely because it centralises, but centralisation converts a local flaw into a systemic exposure. The transferable rule for GS2 and GS3 is that the security standard of a system must rise with the number of people and the sensitivity of the data it aggregates. The examiner rewards the candidate who reads the DPDP Act not as a burden on citizens but as a discipline on data fiduciaries, including the state, and who insists that security-by-design, independent audits, and enforceable breach accountability are the price of a trustworthy digital state.

THE DIAGRAM IN WORDS

```
DPI concentrates many services on one gateway (UMANG) -> efficiency and inclusion at scale -> but concentration magnifies risk -> researchers find architectural flaw, sensitive data (EPFO, Aadhaar) reportedly in plaintext -> exposure surface spans 400 million-plus transactions -> disclosure to MeitY and CERT-In -> fixes applied after the fact -> lesson: security must be designed in, not patched in -> DPDP Act binds data fiduciaries including the state -> remedy: security-by-design, audits, enforceable breach accountability
```

WAY FORWARD

1. **Mandate** (https://ujiyari.com/vocab/mandate/) **security-by-design for DPI.** Government should require encryption at rest, least-privilege access, and independent security audits before any service is onboarded to a shared platform.
2. **Operationalise DPDP breach accountability.** Empower (https://ujiyari.com/vocab/empower/) the Data Protection Board to hold government platforms to the same fiduciary and breach-notification standards as private entities, without carve-outs that dilute citizen protection.
3. **Institutionalise responsible disclosure.** Create clear bug-bounty and coordinated-disclosure channels through CERT-In so that researchers are partners in defence rather than accidental whistle-blowers.
4. **Audit the whole stack, not the app.** Since the flaw lay in the architecture, security reviews must cover the underlying data flows and integrations, not just the front-end service.

PYQ LINKAGE AND PRACTICE

UPSC has asked about cybersecurity, e-governance, and the challenges of digital service delivery. This editorial converts a live disclosure into an applied lesson on securing Digital Public Infrastructure, which is the governance-grade analysis the examiner rewards.

Practice question: "As the state digitalises, cybersecurity becomes a core duty of governance rather than a technical afterthought." Discuss with reference to Digital Public Infrastructure and the obligations of data fiduciaries under the DPDP Act, 2023. (250 words, 15 marks)

Sources: The Hindu (https://www.thehindu.com/), MediaNama (https://www.medianama.com/), Ministry of Electronics and Information Technology (https://www.meity.gov.in/)

Source: The Cracks in the Foundation: UMANG and the Security of Digital Public Infrastructure — Ujiyari.com | Free UPSC & State PCS Editorial Analysis

RELATED DAILY ARTICLES

15 Jul NIA Court Invokes Trial in Absentia Under BNSS Section...

14 Jul Ladakh to Get Autonomous Hill Councils for All Seven...

12 Jul JPC on One Nation One Election Nears Report on the...

11 Jul Supreme Court May Refer 'Written Grounds of Arrest' to...

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/editorials/2026/07/th-umang-portal-data-security-2026/