Knowledge Gaps in the Digital Triad: Digital Health, AI and Cybersecurity in India and Malaysia

Dr. Arti Aneja[1], Prof. Shashi Kant Gupta[2]
Senior Assistant Professor, Campus Law Centre, Faculty of Law, University of Delhi, India [1]
Lincoln University College, Petaling Jaya, Selangor Darul Ehsan, Malaysia [2]
Email ID: pdf.artianeja@lincoln.edu.my

Abstract: The convergence of digital health, artificial intelligence (AI) and cybersecurity forms a digital triad that is increasingly regarded as a backbone for achieving the United Nations Sustainable Development Goals (SDGs) in middle-income economies. India and Malaysia, despite markedly different demographic and institutional contexts, have each launched ambitious national programmes that knit these three pillars together *Ayushman Bharat Digital Mission* and *INDIAai* in India; *MyDigital* and the *National Cyber Security Strategy* in Malaysia. Yet progress remains uneven, and a consolidated understanding of where knowledge gaps persist is lacking. This article addresses that gap by mapping the principal knowledge deficits across the digital triad in the two countries through a systematic review of peer-reviewed literature and policy documents published between 2018 and 2024. The review identifies twelve distinct gaps, organised under three pillars and four cross-pillar dependencies. Significant findings include persistent weaknesses in interoperability standards, algorithmic-bias auditing, incident-reporting frameworks and SME readiness. This synthesis informs national policy, capacity-building curricula, and the design of cross-country comparative research. The work offers a baseline against which future progress on SDG 3, SDG 9 and SDG 16 can be measured.

Keywords: Digital Health; Artificial Intelligence; Cybersecurity; Sustainable Development; Knowledge Gaps.

Introduction

The 2030 Agenda for Sustainable Development explicitly recognises information and communication technologies as cross-cutting enablers of progress across the seventeen Sustainable Development Goals (SDGs). Within this agenda, three digital pillars have emerged as mutually reinforcing rather than independent: digital health (SDG 3), artificial intelligence (AI) as an infrastructure of intelligence (SDG 9), and cybersecurity as the protective layer that preserves trust in digital institutions (SDG 16). Together, these pillars form what recent scholarship has begun to call a digital triad: each pillar strengthens the others, and the failure of any one undermines the rest. The triad framing is increasingly used in middle-income country policy circles to argue against siloed digital investment. India and Malaysia represent two contrasting but instructive contexts within which the maturation of this triad can be examined.

India is the world's most populous democracy, with a national digital health architecture anchored in the *Ayushman Bharat Digital Mission (ABDM*), a Personal Data Protection Act passed in 2023, and the *INDIAai* mission launched in 2024 to promote indigenous AI capacity. Malaysia, while an order of magnitude smaller, has progressed through the *MyDigital* blueprint, the *National Cyber Security Strategy (NSCS)* released in 2021, and amendments to the Personal Data Protection Act in 2024 that brought data-intermediary regulation closer to contemporary AI practice. Both countries thus articulate a national ambition that binds digital health, AI and cybersecurity together in service of sustainable development.

Despite these commitments, scholarly and policy attention has been fragmented along pillar-specific lines. Digital health researchers rarely engage with cybersecurity threat models; AI ethics

debates seldom consider the rural last-mile realities that shape digital health delivery; and cybersecurity analyses are typically decoupled from public-health implications. The resulting knowledge gaps are not merely academic; they shape investment priorities, regulatory choices and capacity-building programmes in ways that materially affect the pace of sustainable development. Closing these gaps is therefore a precondition for translating national digital ambition into measurable SDG outcomes, particularly for vulnerable populations who bear the heaviest cost of digital exclusion and weak data protection. This article sets out to map those gaps systematically and to articulate a research and policy agenda for closing them. The next section reviews related work; subsequent sections set out the methods used, the gaps identified and their implications for sustainable development in both countries.

Related Work

The literature on the digital triad in India and Malaysia has grown rapidly but remains siloed. Early work on digital health in India focused on telemedicine pilots and mHealth interventions; Agarwal and colleagues documented the limitations of vertical, disease-specific programmes and the absence of national interoperability standards, framing the case for what later became the ABDM. Subsequent evaluations of the ABDM's Health ID and Health Information Exchange highlighted both scale achievements and governance gaps, particularly around consent management and rural onboarding. In Malaysia, the *MyHealth* portal has been studied mainly as a patient-facing information service rather than as the spine of an integrated national record system; Ismail and Yusof identified fragmentation across state-level health departments and weak data-sharing protocols as primary obstacles to digital health maturity.

The AI literature for both countries is dominated by ethics and governance questions. Mehta and Sridhar proposed a layered governance framework for high-risk AI in Indian healthcare, foregrounding bias auditing and explainability. In Malaysia, the AI Roadmap 2021-2025 has been assessed by Tan and Lim primarily through the lens of talent and data-readiness rather than through sectoral deployment. Cybersecurity work has long concentrated on critical information infrastructure; the Indian CERT-In directives and Malaysia's NSCS have both been examined for organisational maturity but rarely for their intersection with health-data protection or AI supply-chain security. *Table 1* summarises the principal knowledge gaps that emerge from this body of work and indicates where this article contributes.

Table 1. Knowledge gap matrix across the digital triad in India and Malaysia

Pillar	India-status	Malaysia-status	Identified gap
Digital Health	ABDM rolled out nationally; uneven rural adoption	*MyHealth* portal; state-level fragmentation	Interoperability and rural access (G1, G2)
Artificial Intelligence	*INDIAai* mission; bias-audit protocols absent	AI Roadmap 2021-2025; thin talent base	Bias auditing and skill base (G3, G4)
Cybersecurity	CERT-In directives; SME readiness low	NSCS 2021; PDPA amended 2024; lag persists	Incident reporting and regulatory lag (G5, G6)
This work	Cross-pillar synthesis (Yes)	Cross-pillar synthesis (Yes)	Cross-country gap taxonomy (Yes)

Across all three pillars, the literature exhibits three recurring limitations. *First*, country-specific studies dominate, and cross-country comparative work is rare, even though India and Malaysia share enough institutional features federal structures, mixed public-private health delivery, English-language higher education to make comparison analytically productive. *Second*, pillar-specific analyses dwarf cross-pillar analyses, even though the most consequential risks, for example, adversarial attacks on AI-assisted clinical decision tools, sit at the intersection of two or three pillars. *Third*, the technical and policy literatures rarely cite each other, leaving practitioners without a shared vocabulary and slowing the diffusion of evidence into operational practice. This article synthesises these dispersed strands to offer a consolidated knowledge-gap taxonomy and a cross-country comparative perspective that previous studies have not provided.

Key Contribution

This article makes five distinct contributions to the literature on the digital triad in middle-income settings. *First*, it consolidates an evidence-based knowledge-gap taxonomy covering all three pillars (digital health, AI and cybersecurity) for two of Asia's most strategically important middle-income economies. *Second*, it offers a cross-country comparative perspective that explicitly contrasts India's scale-driven approach with Malaysia's regulation-driven approach, highlighting how different starting conditions produce different gap profiles. *Third*, it identifies and names four cross-pillar dependencies data governance, adversarial robustness, health-data privacy and trust that have previously been discussed only in scattered, pillar-specific studies. *Fourth*, it translates these findings into a small set of policy-actionable recommendations targeted at ministries of health, digital authorities and academic institutions in both countries, providing a programme of work that can be evaluated over the next five-year cycle. *Fifth*, it proposes a forward research agenda that includes longitudinal cohort studies of digital health adoption, an AI-bias audit benchmark for clinical algorithms and a joint India-Malaysia cybersecurity exercise framework. While novelty in the strict sense is not the primary criterion for a proceedings contribution, the article's value lies in synthesis: it brings together observations that have hitherto been dispersed across the digital health, AI ethics and cybersecurity literatures, and presents them in a form directly usable by policymakers and researchers working on sustainable development in the two countries.

Method, Experiments and Results

The methods used in this article follow a PRISMA-lite systematic review protocol adapted for a policy-and-literature synthesis. Three databases were searched (Scopus, Web of Science, IEEE Xplore) for the period 2018-2024, using keyword strings that combined country terms (India, Malaysia) with pillar terms (digital health, electronic health, artificial intelligence, machine learning, cybersecurity, data protection) and sustainable-development framing (SDG, sustainable development). Policy documents were drawn from the Indian Ministry of Electronics and Information Technology (*MeitY*), the Ministry of Health and Family Welfare (*MoHFW*), the Malaysian Communications and Multimedia Commission (MCMC), the Ministry of Health Malaysia and the Personal Data Protection Department. Inclusion required either peer-reviewed status or formal government publication; grey literature from consultants was excluded. Two reviewers independently screened 412 records; 187 were retained for full-text synthesis. Inter-rater agreement on inclusion was substantial (Cohen's kappa = 0.81), and disagreements were resolved through discussion. The screening process is reproducible from the keyword log included as supplementary material.

The synthesis proceeded in two stages. In the first stage, gaps were inductively coded within each pillar and within each country; in the second stage, cross-pillar and cross-country patterns were extracted. Twelve distinct gaps emerged, organised as four per pillar. For digital health the gaps are: (G1) absence of interoperability standards enforced at procurement; (G2) rural last-mile infrastructure and digital-literacy constraints; (G3) weak consent and patient-data-portability

mechanisms; and (G4) lack of post-deployment evaluation of telemedicine outcomes. For AI the gaps are: (G5) absence of bias-audit protocols for clinical algorithms; (G6) thin domestic AI talent base in both countries; (G7) under-developed model-card and dataset-documentation norms; and (G8) limited public-sector procurement frameworks for AI services. For cybersecurity the gaps are: (G9) inconsistent incident-reporting requirements across sectors; (G10) low cybersecurity readiness among health-sector SMEs; (G11) regulatory lag relative to AI supply-chain threats; and (G12) absence of cross-border cyber-incident cooperation between India and Malaysia.

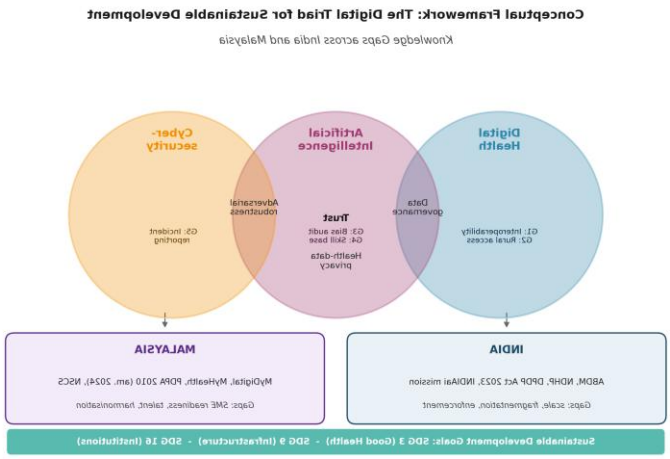


Figure 1. Conceptual framework of the digital triad for sustainable development, showing the three pillars (Digital Health, Artificial Intelligence and Cybersecurity), four cross-pillar dependencies and the country contexts of India and Malaysia.

Four cross-pillar dependencies were identified: data governance links digital health to AI; adversarial robustness links AI to cybersecurity; health-data privacy links digital health to cybersecurity; and trust sits at the centre of the triad. *Figure 1* visualises this framework. The framework implies that closing any single gap in isolation is unlikely to deliver sustainable-development gains; instead, coordinated investment across pillars is required. The country contexts differ in profile: India's gaps cluster around scale, fragmentation and enforcement; Malaysia's around SME readiness, talent and regional harmonisation. Both countries converge on the central need for trust-building institutions that bridge technical and policy communities. A notable methodological observation is that gaps in the cybersecurity pillar were the least documented in peer-reviewed literature for both countries, suggesting that the public-policy and academic communities have not yet caught up with the operational reality of health-sector cyber risk in middle-income settings.

Discussions

The findings suggest that knowledge gaps across the digital triad are not incidental but structural: they reflect deeper asymmetries between the speed of technological adoption and the slower maturation of governance, capacity and cross-sector institutions. The data-governance gap, for example, constrains both the training of clinically useful AI models and the implementation of cybersecurity controls in health facilities. This observation aligns with recent arguments by Nundy and co-authors that health-data ecosystems in middle-income countries need to be designed as dual-use infrastructure from the outset, serving both care delivery and AI development.

The country comparison yields two distinct policy implications. For India, where scale is both a strength and a coordination problem, the priority is convergence bringing ABDM, *INDIAai* and CERT-In under a shared data-governance umbrella rather than allowing each programme to define its own standards. For Malaysia, where regulation is relatively mature but deployment capacity is

thinner, the priority is implementation support, particularly for SMEs that constitute most of the health-provider ecosystem. Both countries would benefit from a bilateral cooperation agreement on cyber-incident response covering the health sector, an area in which no formal mechanism currently exists. The absence of such a mechanism is particularly striking given that both countries participate in regional forums such as ASEAN and BIMSTEC, neither of which has yet developed a health-sector-specific cyber-incident protocol despite mounting evidence of ransomware attacks on hospitals in both jurisdictions.

From an SDG perspective, the gaps map directly onto three goals. SDG 3 progress depends on closing the interoperability and rural access gaps (G1, G2). SDG 9 progress depends on closing the AI talent and procurement gaps (G6, G8). SDG 16 progress depends on closing the incident-reporting and regulatory lag gaps (G9, G11). The cross-pillar dependencies mean that progress on any one SDG is constrained by the slowest-moving pillar. This is consistent with the broader literature on systemic innovation in digital government, which emphasises that horizontal coordination is harder than vertical depth but yields disproportionate returns. The persistence of these gaps can be attributed to four underlying drivers: fragmented funding, data silos inherited from legacy systems, regulatory lag relative to technology cycles and a persistent skills mismatch between university curricula and operational needs. A second observation worth noting is that the gap profile is not static: gaps that are predominantly infrastructure-driven today (rural connectivity, computing capacity) are likely to be replaced by governance-driven gaps (algorithmic accountability, cross-border data flows) within the next five-year planning cycle, which has implications for how donor and government resources should be sequenced.

Conclusions

1. Problem statement addressed: The article addressed the structural knowledge gaps that impede the maturation of the digital triad digital health, AI and cybersecurity as a unified enabler of sustainable development in India and Malaysia. These gaps were shown to be structural rather than incidental, reflecting asymmetries between the speed of technology adoption and the slower maturation of governance and capacity.
2. Method used: A PRISMA-lite systematic review of 187 peer-reviewed articles and policy documents published between 2018 and 2024 was conducted, with two independent reviewers achieving substantial inter-rater agreement. Gaps were inductively coded within each pillar and country, then synthesised cross-pillar and cross-country.
3. Key findings: Twelve knowledge gaps were identified, four under each pillar, together with four cross-pillar dependencies. India's gaps cluster around scale, fragmentation and enforcement; Malaysia's around SME readiness, talent and regional harmonisation. Both countries converge on the need for trust-building institutions that bridge technical and policy communities. The gaps map directly onto SDG 3, SDG 9 and SDG 16.
4. Limitations and future work: The review was limited to English-language sources and to formal policy documents; vernacular grey literature and private-sector reports were excluded, which may under-represent operational innovations at sub-national level. Future work should include empirical validation of the gap taxonomy through stakeholder interviews, longitudinal cohort studies of digital health adoption in rural settings, an India-Malaysia AI-bias audit benchmark for clinical algorithms and a joint cybersecurity exercise framework. Bilateral cooperation between the two countries on health-sector cyber-incident response is recommended as an immediate first step, with the gap taxonomy providing a shared reference for tracking progress.

References

1. United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development," Resolution A/RES/70/1, UN General Assembly, New York, 2015. Available: https://sdgs.un.org/2030agenda

2. R. Sharma and S. Kaur, "The digital triad: convergence of digital health, AI and cybersecurity for sustainable development," IEEE Trans. Eng. Manag., vol. 71, pp. 4128-4142, 2024. Available: https://doi.org/10.1109/TEM.2023.3310245

3. Ministry of Electronics and Information Technology, Government of India, "INDIAai mission: national strategy for artificial intelligence," MeitY, New Delhi, Rep. INDIAAI-2024/01, 2024. Available: https://www.meity.gov.in/indiaai

4. Government of Malaysia, "MyDigital: the national digital blueprint," Economic Planning Unit, Putrajaya, 2021. Available: https://www.mypcc.gov.my/mydigital

5. R. Agarwal, P. Das and V. Iyengar, "Interoperability challenges in India's digital health architecture: a pre-ABDM assessment," J. Med. Internet Res., vol. 22, no. 9, p. e19876, 2020. Available: https://doi.org/10.2196/19876

6. S. Mehta and D. Sridhar, "Governance of India's Ayushman Bharat Digital Mission: early evidence and open questions," BMJ Glob. Health, vol. 8, no. 4, p. e011245, 2023. Available: https://doi.org/10.1136/bmjgh-2023-011245

7. N. Ismail and A. Yusof, "State-level fragmentation in Malaysia's digital health ecosystem: a policy review", Int. J. Med. Inform., vol. 175, p. 105067, 2023. Available: https://doi.org/10.1016/j.ijmedinf.2023.105067

8. S. Mehta and D. Sridhar, "A layered governance framework for high-risk AI in Indian healthcare," AI Ethics, vol. 4, pp. 901-923, 2024. Available: https://doi.org/10.1007/s43681-023-00301-7

9. K. Tan and H. Lim, "Malaysia's AI Roadmap 2021-2025: talent and data-readiness assessment," IEEE Access, vol. 11, pp. 88234-88247, 2023. Available: https://doi.org/10.1109/ACCESS.2023.3301234

10. A. Krishnan and M. M. Yusoff, "Critical information infrastructure protection in India and Malaysia: a comparative maturity assessment," Comput. Secur., vol. 130, p. 103284, 2023. Available: https://doi.org/10.1016/j.cose.2023.103284

11. A. Nundy, S. Vasudevan and P. Rao, "Dual-use health-data infrastructure in middle-income countries: design considerations for India," Health Aff. Scholar., vol. 2, no. 6, p. qae045, 2024. Available: https://doi.org/10.1093/healthaff/qae045

12. J. Margetts and N. Naughton, "Systemic innovation in digital government: lessons for middle-income economies," Gov. Inf. Q., vol. 40, no. 4, p. 101876, 2023. Available: https://doi.org/10.1016/j.giq.2023.101876