Islington Journal of Multidisciplinary Research
Vol. 1, No. 1 | pp. 1–11
Islington College, Kathmandu, Nepal • ISSN 3149-7209 (Online)
Year: 2026

Original Research Article
DOI: 10.67556/e5vr3575

AI Fraud Detection and Financial Trust in Nepals SME Payment Ecosystem: A Readiness Framework

Yogesh Pant[1,*], Aditya Pudasaini[1], Roshan Shrestha[1], Alish K.C.[1]

[1]BSc (Hons) Computing, Islington College, Kathmandu, Nepal
[*]*Correspondence: yogeshpant911@gmail.com*

ARTICLE HISTORY

Received: 5 March 2026 Revised: 8 April 2026
Accepted: 25 May 2026 Published: 08 June 2026

Scan to access

How to Cite (Harvard): Pant et al. (2026). 'AI fraud detection and financial trust in Nepals SME payment ecosystem: A readiness framework', *Islington Journal of Multidisciplinary Research*, 1(1), pp. 1–11. Available at: https://doi.org/10.67556/e5vr3575

ABSTRACT

Nepals rapid transition toward digital payments has outpaced the development of cybersecurity and data-governance infrastructure, leaving small and medium enterprises (SMEs) exposed to rising cyber-enabled fraud and an accompanying deficit of financial trust. Artificial intelligence (AI)-based fraud detection has matured into a standard layer of defense in data-rich financial markets, but these systems rest on assumptions, namely high data maturity, cloud infrastructure, and developed explainability regimes, that do not hold in Nepals fragmented, infrastructure-constrained payment ecosystem. This study conducts a structured integrative review of literature spanning AI-based fraud detection, SME digital trust, and Nepals payment landscape to examine the resulting transferability gap between global AI capabilities and local readiness. Thematic synthesis of the reviewed sources shows that supervised models, behavioral analytics, and graph-based detection cannot be directly transplanted into Nepals context because of data fragmentation, reactive fraud reporting, weak enforcement of Explainable AI (XAI) norms, and acute psychological resistance among merchants. To address this mismatch, the study proposes a five-stage conceptual readiness framework, derived through an explicit gap-to-stage mapping process and assessed through theoretical grounding and comparative benchmarking against existing AI-adoption and maturity models, that sequences data interoperability, unsupervised anomaly detection, economic triage, and XAI compliance ahead of advanced model deployment. The framework offers policymakers, fintech developers, and financial institutions a context-sensitive, trust-centered roadmap for responsible AI-enabled fraud management in Nepal and comparable emerging economies.

Keywords: AI fraud detection, digital payments, financial trust, SMEs

Introduction

Background and Motivation

Over the last five years, Nepals financial system has shifted rapidly from a cash-based to a digital-payment-based economy. The shift accelerated following the COVID-19 pandemic and a series of supportive policies from Nepal Rastra Bank (NRB), the countrys central bank. By mid-2024, mobile banking had reached 24.6 million users, and digital wallets had become commonplace among urban and semi-urban SMEs (Nepal Rastra Bank 2024). For Nepali SMEs, QR-code and mobile-wallet adoption has moved from a competitive advantage to an operational necessity for remaining competitive and accessing credit facilities (Tamang, Bhaskar and Chatterjee 2021).

Globally, the same period has seen AI-based fraud detection mature into a standard layer of financial-crime defense. Supervised classification, unsupervised anomaly detection, behavioral analytics, and graph-based detection are now embedded across financial institutions in data-rich markets (Hilal, Gadsden and Yawney 2022; Hernandez Aros et al. 2024; Nicholls, Kuppa and Le-Khac 2021; Vanini et al. 2023), and supervisory authorities in other emerging markets are actively building internal capacity to monitor AI-related risks, even as that capacity remains uneven across jurisdictions (Crisanto et al. 2024).

Nepals pace of digitalization, however, has consistently outpaced its security and data-governance infrastructure, leaving SMEs exposed to fraud risks they are ill-equipped to absorb. The Financial Intelligence Unit (FIU) has reported that fake payment screenshots, OTP hijacking, and the use of students as money mules account for over 63% of all suspicious transaction reports (Financial Intelligence Unit, Nepal Rastra Bank 2024), and fraud involving digital applications is reported to have increased by 1,225% between 2020 and

2025 (Dhital 2025). For SMEs operating with little margin for error, these schemes are not only a direct financial loss but also erode trust in digital systems, pushing some merchants back toward untraceable cash transactions.

Although major financial institutions worldwide use AI and machine learning to track transactions and flag anomalies in real time, transplanting these solutions into Nepal is not straightforward. AI-based fraud detection of this kind depends on cleanly labeled datasets, cloud computing, and mature regulatory frameworks for explainability, conditions that are presently underdeveloped in Nepal. Deploying such systems prematurely risks generating high false-positive rates that would deepen, rather than resolve, the existing trust deficit (Widayani, Fiernaningsih and Herijanto 2022).

NRB has begun to respond. It has amended its payment-system directives to require incident logging and multi-year business-continuity planning by payment service providers (The Kathmandu Post 2025b), drafted AI-specific guidelines covering fraud detection, credit scoring, and risk management for licensed financial institutions (The Kathmandu Post 2025a), and finalized a Regulatory Sandbox through which new technologies, including AI-based services, can be tested under live supervision (Nepal News 2026). These measures suggest that the regulatory groundwork for AI-enabled fraud detection is beginning to take shape, but they remain early-stage and largely procedural, and do not yet resolve the underlying data fragmentation, infrastructure gaps, and explainability deficits that determine whether AI-based detection can be deployed responsibly.

Scope, Objectives and Research Questions

This paper examines how AI-based fraud detection can be made to work for, rather than against, financial trust and resilience in the digital payments of Nepali SMEs. The scope covers three areas: trends in digital-payment adoption among Nepali SMEs; technical approaches to digital-payment fraud detection available in the literature; and the infrastructural, regulatory, economic, and behavioral factors that determine AI readiness in Nepals payment ecosystem. The study does not involve primary data collection, model building, or model testing; it is bounded to a structured review and conceptual synthesis of existing literature. The empirical scope is geographically limited to Nepal, though international literature is used throughout for comparison and theoretical grounding.

The study is guided by three objectives, each paired with a corresponding research question:

- **Objective 1:** To review the literature on digital payments, fraud detection, and SME financial trust in relation to AI.

  RQ1: What AI-based fraud detection capabilities have been developed in data-mature financial markets, and what assumptions about data, infrastructure, and regulation underlie their effectiveness?
- **Objective 2:** To identify the infrastructural, regulatory, economic, and behavioral readiness challenges affecting AI adoption in Nepals SME payment ecosystem.

  RQ2: What infrastructural, regulatory, economic, and behavioral barriers constrain the transfer of global AI fraud-detection capabilities into Nepals SME digital-payment ecosystem?
- **Objective 3:** To propose a conceptual readiness framework that supports policymakers, fintechs, and financial institutions in moving toward secure, AI-enabled transactions.

  RQ3: How can a phased readiness framework be derived from the identified barriers and validated, within the bounds of a conceptual study, so that it sequences AI adoption in a way that is both technically feasible and trust-preserving for Nepals SMEs?

Research Contribution

This paper makes four primary contributions: (i) It synthesizes global AI-based fraud detection capabilities and evaluates their applicability within Nepals financial ecosystem, (ii) It formally defines and examines the transferability gap associated with deploying AI fraud detection systems in resource-constrained environments, (iii) It proposes a five-stage conceptual readiness framework tailored to low-data, high-risk settings, and (iv) It advances a trust-centered perspective on AI adoption, emphasizing Explainable AI (XAI) and economic feasibility alongside algorithmic performance. (v) It demonstrates a replicable conceptual validation methodology for framework papers in low-resource information-systems contexts, applying theoretical grounding, gap-traceability mapping, and comparative benchmarking as an alternative to empirical validation where primary data collection is outside the study's scope.

Theoretical and Conceptual Foundations

Financial Trust in Digital Ecosystem

Financial trust constitutes the cornerstone of digital payment adoption, reflecting institutional integrity, transaction security, and perceived consumer protection (Rubio and Tulcanaza-Prieto 2025). In developing countries, trust is frequently undermined by historical financial instability, opaque dispute resolution mechanisms, and recurrent cyber incidents. SMEs exhibit heightened trust sensitivity due to thin profit margins, limited risk-bearing capacity, and direct exposure to transaction fraud. Innovation Resistance Theory suggests that psychological barriers including fear, distrust, and perceived loss of control exert a stronger influence on adoption intentions than functional or cost-related factors (Widayani, Fiernaningsih and Herijanto 2022). As a result, technological solutions that appear unclear or make decisions without sufficient transparency may discourage adoption and lead users to revert to cash-based transactions.

AI-Based Fraud Detection Systems

In recent years, AI fraud detection has evolved from traditional rule-based systems to machine learning models capable of analyzing complex patterns within large volumes of transactional data. Supervised models, including Random Forests and Support Vector Machines, rely on extensively labeled historical datasets to classify fraudulent behavior (Hernandez Aros et al. 2024; Dahal, Bhattarai and Karki 2021). However, class imbalance and evolving fraud tactics have spurred interest in unsupervised anomaly detection techniques such as Autoencoders and Isolation Forests, which identify deviations without pre-labeled fraud instances (Hilal, Gadsden and Yawney 2022). Advanced architectures like Graph Neural Networks (GNNs) map relational patterns to detect organized fraud syndicates (Nicholls, Kuppa and Le-Khac 2021). Despite algorithmic sophistication, operational deployment requires deep behavioral session tracking, low-latency API integration, and economic triage models to balance detection accuracy with investigation costs (Vanini et al. 2023; Karki 2012). Importantly, the opacity of deep learning models is inconsistent with regulatory demands for transparency and user trust. Therefore, this necessitates Explainable AI (XAI) frameworks such as LIME and SHAP (Gupta 2024; Hilal, Gadsden and Yawney 2022).

Technology Readiness and Socio-Technical System

The adoption of AI is not just about technical feasibility since it occurs within socio-technical systems characterized by interrelated elements such as the infrastructure, regulations, human resources, and organizational cultures. The theory of socio-technical systems suggests that technical success requires matching the capabilities with the social and organizational context. Readiness assessments include the analysis of maturity in data, interoperability requirements, computing capabilities, and enforcement (Hilal, Gadsden and Yawney 2022; Vanini et al. 2023). Emerging markets lack adequate AI governance, as they have no mandates in place for issues like algorithmic auditability, privacy, and consumer redress programs (Crisanto et al. 2024; Nicholls, Kuppa and Le-Khac 2021). The innovation resistance theory additionally highlights the role of the fear of complexity and insecurity, as well as institutional lack of accountability, in constraining innovation (Widayani, Fiernaningsih and Herijanto 2022; Rubio and Tulcanaza-Prieto 2025).

Review Methodology

Research Design and Rationale for an Integrative Review

This study adopts a structured integrative literature review, a design developed for synthesizing theoretical, empirical, and institutional sources into new conceptual knowledge, rather than aggregating quantitative findings from a methodologically homogeneous body of studies (Torraco 2016; Whittemore and Knafl 2005). An integrative review is appropriate here for two reasons. First, the literature spanning AI-based fraud detection, SME digital trust, and Nepals payment ecosystem is disciplinarily heterogeneous, spanning machine-learning evaluation studies, behavioral-adoption surveys, and institutional or regulatory reports, a mix that does not lend itself to the structured quantitative aggregation used in systematic or meta-analytic reviews. Second, the studys objective is theory-building rather than effect-size estimation: the aim is to construct a new conceptual framework by mapping global AI capabilities against Nepals local realities, which is precisely the kind of generative, cross-domain synthesis the integrative review method is designed to support (Torraco 2016). This contrasts with closely related systematic reviews in similar contexts, such as Ampumuza, Katushabe and Tamale (2026), which are designed primarily to catalogue existing detection methods. Because our objective is to construct a novel conceptual framework rather than merely inventory current tools, we require the broader interpretive synthesis that an integrative design affords.

Data Source and Search Strategy

Literature was drawn from international academic databases (IEEE Xplore, ScienceDirect, SpringerLink, and MDPI), global institutional repositories (including the World Bank Global Findex Database), and localized Nepali institutional sources (Nepal Rastra Bank publications, FIU-Nepal strategic reports, and Nepal Journals Online). During revision, this base was supplemented with recent regulatory and methodological sources, including Bank for International Settlements FSI Insights papers and Nepal Rastra Bank circulars and directives reported through 2026, to capture developments that postdate the original search and to strengthen the methodological grounding requested in review. Search terms combined the core constructs under study (for example, AI fraud detection, SME digital trust, Nepal digital payment, Explainable AI finance, AI readiness framework), adapted to each databases syntax.

Scope and Analytical Lens

Sources were included if they were peer-reviewed or institutionally authoritative (a central bank, financial intelligence unit, or international financial-sector body), published between 2018 and 2026, and substantively addressed fraud, financial trust, AI/ML-based detection, or SME digital-payment adoption. Sources were excluded if they addressed AI fraud detection in technical isolation from any deployment or adoption context, or if they fell outside the 20182026 window without continued citation relevance. The original draft synthesized fifteen core sources across these domains. However, to strengthen the paper and address requests for a broader literature base, we significantly expanded this pool during the revision process. We added twelve new sources, incorporating recent global AI-adoption frameworks, low-resource fraud models, and the latest regulatory updates from Nepal, alongside key methodology papers to justify our review design. The final analysis is now supported by a robust, well-rounded pool of twenty-seven sources.

Analytical Process: From Literature to Framework

The 5-Stage Phased Readiness Framework presented in Section 5 was not asserted a priori, it was derived from the literature through a three-step analytical process.

First, open coding was applied to the retained sources to identify recurring constructs across three domains: (i) the technical capabilities and data/infrastructure assumptions of global AI fraud-detection systems; (ii) the structural and regulatory characteristics of Nepals payment ecosystem; and (iii) the behavioral and psychological determinants of SME trust in digital systems.

Second, axial coding grouped these open codes into five recurring barrier categories that appeared independently across the technical, local-context, and adoption literatures: data maturity and interoperability; infrastructure and connectivity; regulatory frameworks and enforcement (including XAI); human capital and digital literacy; and economic viability and cost optimization. These five categories structure the readiness analysis presented in Section 4.3 and are each separately traceable to specific cited sources (see Table 3 in Section 6.3).

Third, each barrier category was translated into a corresponding intervention stage, and the five resulting stages were sequenced according to technical and institutional dependency rather than by the order in which the barriers were identified in the literature. Basic digitization and cyber-safety (Stage 1) were placed first because the literature indicates that without baseline platform reliability and merchant awareness, neither systematic data collection nor trust-building can proceed (Widayani, Fiernaningsih and Herijanto 2022; Gupta 2024). Data readiness and interoperability (Stage 2) precede algorithmic deployment because supervised and even most unsupervised techniques require some minimum of structured, aggregated transaction data, which the literature shows Nepal currently lacks (Pathak 2024; Financial Intelligence Unit, Nepal Rastra Bank 2024). Unsupervised detection and economic triage (Stage 3) is positioned before advanced model deployment because the absence of labeled fraud data forecloses supervised learning in the near term, while economic triage is required to keep false-positive costs proportionate to SME transaction values (Hilal, Gadsden and Yawney 2022; Vanini et al. 2023). AI implementation and XAI compliance (Stage 4) follows because the regulatory-readiness literature indicates that explainability cannot be retrofitted onto opaque models after deployment without undermining trust (Nicholls, Kuppa and Le-Khac 2021; Dhital 2025). Trust-building and ecosystem scaling (Stage 5) is positioned last because it is the outcome the preceding four stages are designed to produce, rather than a precondition for them, consistent with Innovation Resistance Theorys account of trust as a cumulative product of repeated, transparent, low-harm interactions (Widayani, Fiernaningsih and Herijanto 2022; Rubio and Tulcanaza-Prieto 2025).

This derivation logic, mapping each stage to a literature-identified barrier and ordering stages by dependency rather than by narrative convenience, is the basis for the framework-validation procedures described in Section 6.

The literature evidence supporting each of these sequencing decisions is presented in full in Section 4; the present section establishes the process by which they were generated. Readers encountering the barrier citations above before reading Section 4 may treat them as forward references they are intended as a preview of the evidential basis that Section 4 elaborates.

Literature Review and Related Work

Nepals SME Digital Payment Ecosystem

Nepals transition to digital payments accelerated through pandemic-era avoidance of physical currency and NRB policies promoting QR-code and wallet interoperability (Tamang, Bhaskar and Chatterjee 2021). Adoption among individual users has been strong, but SMEs continue to face structural inefficiencies. The absence of a universal switch connecting financial institutions and payment service providers (PSPs) prevents data interoperability across the ecosystem (Pathak 2024), and some merchants continue to rely on physical cash because of unreliable power and internet connectivity, particularly outside major urban centers (Anakpo, Xhate and Mishi 2023; Klapper et al. 2025).

Global AI Fraud Detection Capabilities and the Transferability Gap

International financial institutions rely on a layered set of AI techniques: supervised models trained on historical fraud labels, unsupervised anomaly detectors such as Autoencoders and Isolation Forests for previously unseen fraud patterns, Graph Neural Networks for mapping fraud-ring relationships, behavioral analytics drawing on device and session data, and economic triage models that adjust detection thresholds to transaction value (Hilal, Gadsden and Yawney 2022; Hernandez Aros et al. 2024; Nicholls, Kuppa and Le-Khac 2021; Vanini et al. 2023). Increasingly, these systems are paired with Explainable AI methods, such as LIME and SHAP, to satisfy regulatory demands for transparency (Gupta 2024; Hilal, Gadsden and Yawney 2022).

These capabilities, however, assume conditions, mature labeled data, low-latency cloud infrastructure, advanced XAI enforcement, and a trained data-science workforce, that do not hold in Nepal. The transferability gap, defined here as the difference between the technical assumptions of global AI fraud detection and the infrastructural, regulatory, and behavioral realities of developing-country payment systems, manifests along five dimensions: data cohesion; connectivity and computing capacity; regulatory enforcement of explainability; cybersecurity awareness; and tolerance for false-positive cost. Table 1 maps each of these dimensions against Nepals current reality.

Readiness Analysis: Mapping AI Capabilities Against Nepals Reality

Table 1 summarizes the mismatch between global AI requirements and Nepals payment-ecosystem realities across the five barrier dimensions identified through the analytical process described in Section 3.4.

Table 1: Readiness Gap Analysis

Dimensions	Global AI Requirement	Nepal's Current Reality	Key Sources
Data Maturity & Interoperability	More than 100 behavioral features per session, centrally aggregated, well-labeled transaction histories	Fragmented data across non-interoperable PSPs; reactive detection triggered only by victim reports; no centralized record of recurring fraud typologies such as Re. 1 test-debit probing	Vanini et al. (2023); Pathak (2024); Financial Intelligence Unit, Nepal Rastra Bank (2024)
Infrastructure & Connectivity	Low-latency cloud computing and API integration for real-time scoring	Urban connectivity has improved, but semi-urban and rural areas lack reliable power and internet, limiting real-time deployment	Hilal et al. (2022); Tamang et al. (2021); Klapper et al. (2025)
Regulatory Frameworks & Enforcement	Enforceable XAI mandates, algorithmic auditability, privacy-by-design rules	Strong legislative intent (regulatory sandbox, draft AI guideline, directive amendments) but limited enforcement capacity for XAI and KYC violations	Nicholls et al. (2021); Dhital (2025); The Kathmandu Post (2025; 2025b); Nepal News (2026)
Human Capital & Digital Literacy	Skilled data-science talent; forensic capacity to validate flagged cases	Workforce skill gaps compounded by widespread cybersecurity-awareness gaps among merchants, raising susceptibility to social engineering	Vanini et al. (2023); Gupta (2024); Widayani et al. (2022)
Economic Viability & Cost Optimization	Cost-optimized thresholds balancing investigation expense against fraud loss, sustainable at enterprise scale	Thin SME margins make high false-positive rates economically punishing and likely to drive reversion to cash	Vanini et al. (2023); Irianto & Chanvarasuth (2025); Klapper et al. (2025); Anakpo et al. (2023)

Two implications follow from this mapping. First, the dimensions are not independent: data fragmentation (dimension 1) is itself partly a consequence of weak enforcement (dimension 3), since no directive currently compels PSPs to share standardized transaction logs. Second, the dimension most resistant to short-term intervention, human capital and digital literacy, is also the one most directly responsible for the social-engineering fraud patterns described in Section 4.1, which suggests that technical fixes alone, however sophisticated, cannot resolve the trust deficit without parallel investment in merchant education.

Related Work: Positioning This Study Among Existing Literature Streams

Table 2 positions this study against five distinguishable literature streams that, between them, cover most of the ground this paper draws on.

Table 2: Positioning Relative to Related Work

Literature Stream	Representative Studies	Focus	Limitation Relative to This Study
Global technical AI fraud-detection literature	Hilal et al. (2022); Hernandez Aros et al. (2024); Nicholls et al. (2021); Vanini et al. (2023)	Algorithmic capability and accuracy (supervised, unsupervised, GNN, XAI) in data-rich settings	Assumes data and infrastructure maturity; does not address transferability to low-resource markets
Nepal-specific cyberfraud and cybersecurity literature	Dhital (2025); Financial Intelligence Unit, Nepal Rastra Bank (2024); Gupta (2024)	Documents the scale and typology of cyber-enabled fraud in Nepal	Recommends reactive and awareness-based measures; does not propose an algorithmic or phased adoption pathway
SME digital-trust and adoption-barrier literature	Widayani et al. (2022); Rubio & Tulcanaza-Prieto (2025); Irianto & Chanvarasuth (2025)	Psychological and behavioral barriers to digital-payment adoption	Does not examine how algorithmic opacity specifically compounds these barriers
TOE-based AI-adoption literature	Badghish & Soomro (2024)	Identifies organizational, technological, and environmental determinants of general AI adoption by SMEs	Explains why SMEs adopt AI broadly, but offers no sequencing logic for fraud-specific, trust-sensitive deployment
Low-resource hybrid fraud-detection frameworks	Ampumuza et al. (2026)	Systematic review proposing a hybrid AI–audit model for fraud detection in resource-constrained cooperative finance (Uganda SACCOs)	Proposes a technical hybrid model but does not stage deployment by infrastructural/regulatory readiness or treat XAI as a gating compliance mechanism

Taken together, these five literature streams converge on, but do not resolve, the problem motivating this study. They establish that the technical capability exists, that Nepals fraud problem exists, that trust barriers exist, and that general AI adoption can be explained through TOE-type determinants; none of them, however, proposes a sequencing logic that connects these strands into a deployment pathway oriented specifically toward fraud detection and toward defusing, rather than risking, SME trust through staged use of explainability and economic triage.

The Research Gap

Synthesizing Sections 4.1 to 4.4 surfaces a gap that no single literature stream addresses on its own. The global technical literature (Hilal, Gadsden and Yawney 2022; Vanini et al. 2023; Hernandez Aros et al. 2024) consistently recommends complex supervised algorithms that require large volumes of labeled data and substantial cloud infrastructure, conditions absent in developing countries such as Nepal; several of these studies explicitly call for further research into unsupervised algorithms suited to data-scarce environments. The Nepal-specific literature (Dhital 2025; Financial Intelligence Unit, Nepal Rastra Bank 2024; Gupta 2024) documents the scale of the problem convincingly but stops at reactive recommendations, faster reporting and awareness campaigns, without exploring proactive, algorithmic alternatives. The SME trust and adoption literature (Widayani, Fiernaningsih and Herijanto 2022; Rubio and Tulcanaza-Prieto 2025; Irianto and Chanvarasuth 2025) identifies real psychological barriers to digital-payment adoption but does not examine how introducing opaque, black-box AI models could deepen exactly the trust deficit these studies describe. Closer to a technical solution, TOE-based adoption studies (Badghish and Soomro 2024) and low-resource hybrid detection frameworks (Ampumuza, Katushabe and Tamale 2026) come nearer to this studys territory, the first by modeling why SMEs adopt AI, the second by proposing a technical model for fraud detection under resource constraints, but neither sequences deployment according to infrastructural and regulatory readiness, nor treats explainability and trust as the organizing logic of that sequence.

The gap that remains, once all five streams are read together, is the absence of any framework connecting global AI capability to Nepals infrastructural, regulatory, and behavioral reality in a way that gives policymakers, fintechs, and financial institutions a concrete, ordered pathway from reactive fraud management to proactive, trust-preserving AI adoption. This paper addresses that gap through the 5-Stage Phased Readiness Framework. Following Hilal et al.s (2022) call to study unsupervised techniques in previously data-scarce settings, the framework offers a definite roadmap that begins with data preparedness and culminates in XAI-compliant deployment, tailored specifically to Nepals digital-payment context.

Proposed Conceptual Readiness Framework

The readiness gap synthesized in Section 4.5 reveals that Nepal's digital payment ecosystem cannot support the direct deployment of the AI fraud detection capabilities described in Section 4.2. The five barrier dimensions identified in Table 1 data fragmentation, infrastructure constraints, weak XAI enforcement, digital-literacy deficits, and thin SME margins are not isolated problems; they are interdependent preconditions that must be addressed in a specific order before advanced algorithmic systems can function without generating the false positives and trust erosion that would undermine adoption. The following framework proposes that sequence.

The 5-Stage Phased Readiness Model

Addressing the gap mentioned above involves abandoning a "plug and play" paradigm in AI implementation. Rather, this paper proposes a 5-stage phased readiness model specific to the digital payment environment in Nepal. The framework represents the key theoretical contribution of this research paper, as each stage builds upon the previous one (Figure 1).

- **Stage 1: Basic Digitization & Cyber-Safety**
  Before leveraging AI, it is imperative to lay the foundation and ensure that the baseline is secured. This will involve ensuring increased tech support in rural regions and the creation of platform-specific awareness campaigns on social engineering and QR code manipulation. At this step, trust will be gained via the basics such as reliability and training.
- **Stage 2: Data Readiness & Interoperability**
  National data formatting requirements must be agreed upon by the regulators and PSPs. Data interoperability will lead to the creation of a platform where localized fraud typologies can be aggregated to be used for training supervised models.
- **Stage 3: Unsupervised Detection & Economic Triage**
  Due to the current lack of labels, PSPs should utilize an unsupervised anomaly detection system such as Isolation Forests. By adjusting the detection threshold according to the value of the transaction, unnecessary costs related to the processing of false positives in SME transactions can be avoided.
- **Stage 4: AI Implementation & XAI Compliance:**

  With adequate levels of data maturity attained, the organizations can experiment with cutting-edge technologies, like Graph Neural Networks for identifying money mule associations. It is essential that these experiments be carried out in the NRB's regulatory sandbox and in accordance with Explainable AI (XAI) methodologies. In the case that the transaction of an SME is rejected, an explanation must be provided to avoid causing psychological harm due to a "black box" outcome.
- **Stage 5: Building Trust & Scaling the Ecosystem**

  The last stage shifts from protecting from fraud to actively building trust. Given that the use of AI technologies proves effective in reducing financial loss and speeding dispute resolution, confidence in these technologies grows. Increased trust in turn leads to financial inclusivity and transition from the cash-based informal economy.

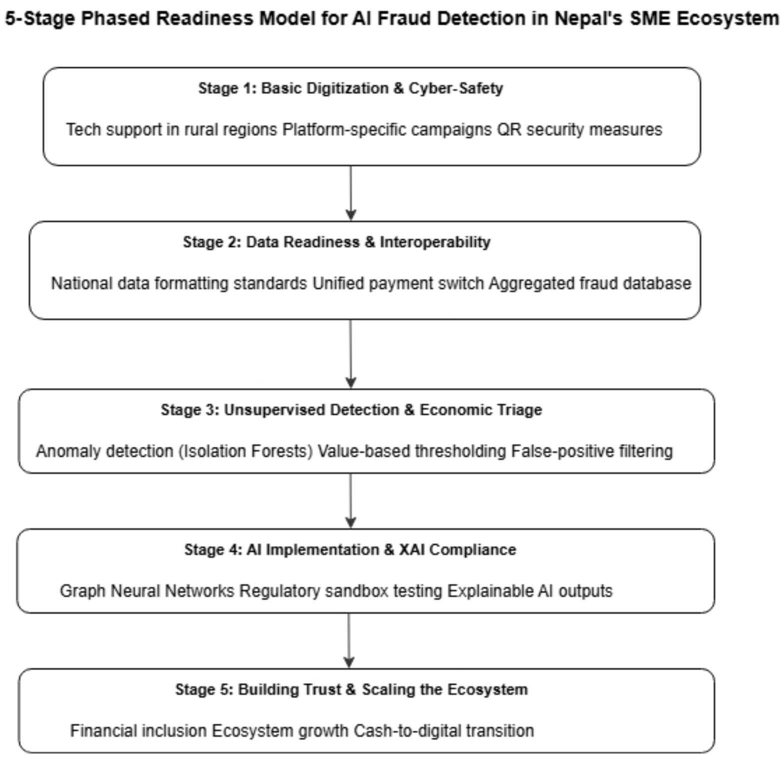

Figure 1: 5-Stage Phased Readiness Model for AI Fraud Detection in Nepal's SME Digital-Payment Ecosystem

Framework Validation

Validation Approach for Conceptual Frameworks

Frameworks of this kind are most rigorously validated through structured expert-consensus methods such as the Delphi technique, in which a panel of subject-matter experts iteratively reviews and refines a proposed model until consensus is reached (J. Skulmoski, T. Hartman and Krahn 2007). Recent examples in adjacent conceptual-framework research illustrate the approach: Manzini et al. (2026) validated a systems-based organizational-resilience framework through a two-round Delphi process with a multidisciplinary expert panel, reaching high consensus on the frameworks structure before recommending it for practical use. Because the present study is explicitly conceptual, built on literature synthesis rather than primary data collection, a full Delphi panel falls outside its current scope; conducting one is identified in Section 8 as the appropriate next methodological step before any pilot implementation. Within the bounds of a conceptual study, however, validity can and should still be demonstrated through methods that interrogate the frameworks grounding and positioning rather than its real-world performance. This study uses three such methods: theoretical grounding, gap-traceability mapping, and comparative benchmarking against existing frameworks.

Theoretical Grounding

The framework's internal validity is grounded in the two theoretical lenses underpinning this study. Rather than applying competing theories to cross-check findings, which triangulation proper requires, this study uses IRT and STST as complementary analytical anchors that together account for all five stages at different levels of analysis. Innovation Resistance Theory accounts for Stage 1 (basic digitization and cyber-safety) and Stage 5 (trust-building), since the theory holds that psychological barriers, fear, distrust, and perceived loss of control, are addressed first by establishing reliability and only later resolved through demonstrated, repeated benefit (Widayani, Fiernaningsih and Herijanto 2022). Socio-Technical Systems Theory accounts for Stages 2 through 4, since it holds that technical capability (data infrastructure, algorithms, XAI tooling) must be matched to social and organizational context, here, regulatory enforcement capacity and merchant-level digital literacy, before deployment can succeed. No stage in the framework relies on a theoretical assumption that is not already established in Section 2, supporting the frameworks internal theoretical coherence.

Gap-Traceability Validation

A second test of validity is whether each stage can be traced transparently back to a specific, cited deficiency identified in the literature review, rather than being introduced without evidentiary grounding. Table 3 demonstrates this traceability.

Table 3: Stage-to-Gap Traceability

Framework Stage	Literature-Identified Barrier Addressed	Supporting Sources
Stage 1: Basic Digitization & Cyber-Safety	Human-capital and digital-literacy gap; social-engineering susceptibility	Widayani et al. (2022); Gupta (2024)
Stage 2: Data Readiness & Interoperability	Data fragmentation; absence of a universal payment switch	Pathak (2024); Financial Intelligence Unit, Nepal Rastra Bank (2024)
Stage 3: Unsupervised Detection & Economic Triage	Absence of labeled fraud data; thin SME margins and false-positive intolerance	Hilal et al. (2022); Vanini et al. (2023); Irianto & Chanvarasuth (2025)
Stage 4: AI Implementation & XAI Compliance	Weak enforcement of explainability and auditability mandates	Nicholls et al. (2021); Dhital (2025); The Kathmandu Post (2025; 2025b)
Stage 5: Building Trust & Scaling	Cumulative trust deficit; reversion to cash	Rubio & Tulcanaza-Prieto (2025); Widayani et al. (2022)

Each stage maps to at least one literature-identified barrier, with no stage left unsupported by the review and no major barrier identified in Section 4.3 left unaddressed by any stage, indicating that the frameworks scope is neither under- nor over-specified relative to the reviewed evidence.

Comparative Benchmarking Against Existing Frameworks

A third validation step benchmarks the framework's structure against three classes of existing models: generic AI-maturity models used in enterprise settings, TOE-based AI-adoption models, and low-resource hybrid fraud-detection frameworks. This comparison evaluates whether the proposed framework occupies a distinct, non-redundant position in the landscape of existing readiness and maturity models, a recognized technique for establishing the validity of a new conceptual contribution (Torraco 2016).

Generic AI maturity models, such as those published by Gartner (2026) and MIT Sloan Management Review (2026), are designed to benchmark organization-wide AI capability across a firm's entire technology portfolio. They are sector-agnostic, assume an enterprise IT baseline that is largely absent in Nepal's SME sector, and treat governance as one maturity dimension among several rather than as a sequenced precondition. They do not address infrastructure-poor deployment contexts, nor do they model trust or explainability as terminal outcomes.

TOE-based AI adoption models, represented here by Badghish and Soomro (2024), explain the organizational, technological, and environmental determinants of AI adoption decisions by SMEs. Their contribution is explanatory rather than prescriptive they identify why adoption occurs but offer no sequencing logic for the order in which technical preconditions should be satisfied, particularly in fraud-sensitive, trust-critical deployment scenarios.

Low-resource hybrid fraud-detection frameworks, such as Ampumuza, Katushabe and Tamale (2026), address resource-constrained contexts directly by proposing a hybrid AIaudit model for fraud detection in cooperative finance. However, this framework proposes a technical architecture without staging its deployment according to infrastructural or regulatory readiness, and does not treat XAI compliance as a gating mechanism that must precede advanced model deployment. Applying such a framework to Nepal's context without first completing Stages 1 and 2 of the proposed model basic digitization and data interoperability would result in deploying detection algorithms against fragmented, non-standardized transaction data, producing the high false-positive rates that Section 4.3 identifies as the primary trust-destruction mechanism for thin-margin SMEs.

Taken together, this comparison confirms that the proposed 5-Stage Phased Readiness Framework occupies a distinct position in the existing landscape: it is the only model among those reviewed that simultaneously sequences deployment by infrastructural and regulatory readiness, treats economic triage and XAI compliance as ordered preconditions rather than optional features, and positions trust as the terminal output of the entire deployment sequence rather than a background assumption. A full comparative analysis across these dimensions is presented in Table 4 in Section 7.1.

Results and Discussion

Comparative Analysis with Existing Frameworks

Table 4 compares the proposed 5-Stage Readiness Framework with three classes of existing models that address related, but distinct, problems.

Table 4: Comparative Analysis of Readiness and Adoption Frameworks

Feature	This Study (5-Stage Readiness Framework)	Generic AI Maturity Models *(Gartner, 2026; MIT Sloan Management Review, 2026)*	TOE-Based AI Adoption Models *(Badghish & Soomro, 2024)*	Low-Resource Hybrid Fraud Frameworks *(Ampumuza et al., 2026)*
Primary purpose	Sequence fraud-detection deployment by infrastructural and regulatory readiness	Benchmark organization-wide AI capability	Explain determinants of AI-adoption decisions	Propose a technical hybrid detection model
Sector specificity	Fraud detection in SME digital payments	Sector-agnostic	Sector-agnostic (general AI)	Cooperative and low-resource finance
Sensitivity to infrastructure-poor settings	Explicit; the central organizing logic	Largely absent; assumes an enterprise IT baseline	Partial; environment is one of three TOE pillars, not central	Present, but framed around audit/technical hybridity rather than staged readiness
Treatment of trust and explainability	XAI compliance is a sequenced gate; trust is the terminal outcome	Governance is one maturity dimension among several	Not directly modeled	Not addressed
Validation status	Theoretical grounding, gap-traceability mapping, and comparative benchmarking (this paper); Delphi panel recommended as next step	Industry-developed, practitioner-validated	Empirically tested via SME survey data	Systematic synthesis

Novelty and Advantages

The proposed frameworks distinguishing contribution is that it treats readiness as a sequence rather than a score, and treats trust as the frameworks terminal output rather than a background condition. Unlike generic AI maturity models, which assume an enterprise IT baseline largely absent in Nepals SME sector, or TOE-based adoption models, which explain why adoption happens but not in what technical order it should happen, the 5-Stage framework provides ordered, actionable guidance for a fraud-detection use case in which false positives carry outsized reputational and trust costs for thin-margin SMEs. Relative to low-resource hybrid detection frameworks such as Ampumuza, Katushabe and Tamale (2026), the present frameworks distinguishing feature is its explicit staging logic, technical capability is deliberately withheld until the infrastructural and regulatory preconditions for its responsible use are in place, rather than proposed independently of readiness.

Implications

Theoretical Implications

This study extends Innovation Resistance Theory and Socio-Technical Systems Theory by demonstrating how algorithmic opacity and infrastructural fragmentation jointly suppress AI adoption in emerging markets. It introduces the transferability gap as a conceptual lens for evaluating technology-deployment mismatches, and demonstrates, through Sections 6 and 7.1, how a conceptual framework of this kind can be validated and positioned without primary data collection.

Physical Implications

Policymakers can use the framework to prioritize data standardization, sandbox testing, and XAI mandates before incentivizing advanced AI procurement. Fintech developers should focus on lightweight unsupervised models and explainability modules rather than resource-intensive deep-learning architectures. Financial institutions can implement economic triage to optimize fraud-investigation costs while preserving SME operational continuity.

Policy Implications

NRB and other regulatory bodies should institutionalize data-sharing standards, mandate algorithmic transparency for financial AI, and expand cybersecurity-literacy programs targeted at merchant populations. International development partners can support connectivity expansion and cloud-infrastructure subsidies to reduce the digital divide. Notably, NRBs recent Regulatory Sandbox and draft AI guideline (Nepal News 2026; The Kathmandu Post 2025a) provide exactly the kind of supervised-testing mechanism Stage 4 anticipates, suggesting that the institutional groundwork for the frameworks later stages is beginning to emerge even as this framework was being developed and revised.

Limitations and Future Research

This study has several limitations that should be acknowledged.

- **Conceptual Nature:** The research relies on integrative literature synthesis rather than empirical data collection, algorithmic testing, or pilot implementation. Consequently, the proposed 5-Stage Phased Readiness Framework has not undergone real-world validation within Nepals SME digital-payment ecosystem.

- **Validation Gap:** Section 6 validates the framework conceptually, through theoretical grounding, gap-traceability mapping, and comparative benchmarking, but a structured Delphi panel of regulators, fintech practitioners, and SME representatives (J. Skulmoski, T. Hartman and Krahn 2007) remains the recommended next step to establish expert consensus on the frameworks content validity before any pilot implementation.
- **Context Specificity:** The framework is tailored to Nepals particular infrastructural, regulatory, and behavioral context; direct transferability to other emerging economies requires further comparative analysis.
- **Data Constraints:** The analysis depends on publicly available institutional reports and peer-reviewed literature; proprietary transaction data from Nepali PSPs or banks was not accessible for model-training simulations.
- **Future Research Directions:** To address these limitations, future work should prioritize the following.
  - **Expert Panel Validation:** Convene a structured Delphi panel of NRB representatives, fintech developers, and SME merchants to formally validate the frameworks content and structure ahead of pilot work.
  - **Pilot Testing:** Collaborate with three to five Nepali payment service providers to evaluate Stage 3 unsupervised-detection performance on anonymized real-world transaction data.
  - **Stakeholder Validation:** Conduct semi-structured interviews with policymakers, fintech developers, and SME merchants to assess perceived usability, trust implications, and adoption barriers for each framework stage.
  - **Simulation Modeling:** Develop agent-based or economic simulations to quantify the impact of false-positive reduction via value-based thresholding (Stage 3) and XAI-compliant explanations (Stage 4).
  - **Cross-Country Comparison:** Extend the transferability-gap analysis to similar emerging economies (for example, Bangladesh, Sri Lanka, Kenya) to refine the frameworks generalizability.

Conclusion

The rapid digitization of Nepals financial sector has outpaced the development of defensive security infrastructure, creating a pronounced trust deficit among SMEs exposed to localized cyber-enabled fraud. While global financial institutions successfully leverage AI for real-time fraud detection, direct transplantation into Nepals fragmented, infrastructure-constrained, and trust-sensitive environment remains unviable.

Based on a structured integrative literature review, this study identifies a critical transferability gap and proposes a five-stage conceptual readiness framework, derived transparently from literature-identified barriers and validated through theoretical grounding, gap-traceability mapping, and comparative benchmarking against existing AI-adoption and maturity models. Rather than prioritizing technological implementation, the model emphasizes ecosystem maturation. The findings demonstrate that data interoperability, economic triage, and Explainable AI (XAI) compliance must precede advanced machine learning deployment to preserve merchant confidence and prevent operational disruption.

Returning to the three research questions that guided this study: RQ1 is addressed in Section 4.2, which establishes that global AI fraud detection relies on supervised models, unsupervised anomaly detectors, GNNs, and XAI frameworks, all of which assume data maturity, cloud infrastructure, and regulatory enforcement absent in Nepal. RQ2 is addressed through the five barrier dimensions in Table 1, which show that data fragmentation, infrastructure gaps, weak XAI enforcement, digital-literacy deficits, and thin SME margins collectively prevent direct transplantation of these capabilities. RQ3 is addressed by the derivation process in Section 3.4 and the three-method validation in Section 6, which together demonstrate that a phased sequence beginning with data interoperability and culminating in XAI-compliant deployment is both technically feasible and trust-preserving for Nepal's SME context.

These insights carry direct implications for stakeholders. For the Nepal Rastra Bank and regulatory bodies, the immediate priority should be institutionalizing data-sharing standards and expanding regulatory sandboxes for XAI-compliant model testing. FinTech developers and commercial banks should focus on lightweight unsupervised anomaly detection and value-based transaction thresholding, rather than deploying resource-intensive algorithms that exceed current infrastructural capacity.

Ultimately, artificial intelligence cannot function as a standalone solution to Nepals digital fraud challenge. Its effectiveness depends entirely upon sequential infrastructure development, regulatory clarity, and sustained institutional trust.

Disclosure Statement

The authors have no financial or non-financial disclosures to share for this article.

Ethical Approval: Not applicable.

Consent to Participate: Not applicable.

Consent to Publish: Not applicable.

Data Availability Statement: This research used already existing data from different sources. All of them have been cited as well.

Use of Artificial Intelligence (AI) Tools: This research utilized AI to improve the language as well as finding minor grammatical errors. The ideas, analysis, and argument are the authors' own.

Authors' Contributions: Yogesh Pant contributed to conceptualization, literature synthesis, framework development, manuscript drafting, and data analysis. Aditya Pudasaini contributed to methodology design, literature review, critical revision, and formatting compliance. Roshan Shrestha contributed to academic supervision, scope refinement, and editorial guidance. Alish K.C. contributed to research validation, theoretical framing, and final manuscript review. All authors read and approved the final version of the manuscript.

Funding: No funding was received.

Conflict of Interest: All authors have no competing interests.

Acknowledgement

The authors thank Islington College for institutional support and academic resources provided during the preparation of this manuscript.

References

Ampumuza, Dalton, Calorine Katushabe and Micheal Tamale (Jan. 2026). "A systematic review and future directions for AI-driven detection of fraud patterns in SACCO transactions." In: *Frontiers in Artificial Intelligence* 8. ISSN: 2624-8212. 10.3389/frai.2025.1690482. http://dx.doi.org/10.3389/frai.2025.1690482.

Anakpo, Godfred, Zizipho Xhate and Syden Mishi (2023). "The Policies, Practices, and Challenges of Digital Financial Inclusion for Sustainable Development: The Case of the Developing Economy." In: *FinTech* 2.2, pp. 327–343. ISSN: 2674-1032. 10.3390/fintech2020019. http://dx.doi.org/10.3390/fintech2020019.

Badghish, Saeed and Yasir Ali Soomro (Feb. 2024). "Artificial Intelligence Adoption by SMEs to Achieve Sustainable Business Performance: Application of TechnologyOrganizationEnvironment Framework." In: *Sustainability* 16.5, p. 1864. ISSN: 2071-1050. 10.3390/su16051864. http://dx.doi.org/10.3390/su16051864.

Crisanto, Juan Carlos, Cris Benson Leuterio, Jermy Prenio and Jeffery Yong (Dec. 2024). *Regulating AI in the Financial Sector: Recent Developments and Main Challenges*. FSI Insights on Policy Implementation 63. Basel: Bank for International Settlements, Financial Stability Institute. https://www.bis.org/fsi/publ/insights63.pdf.

Dahal, Rewan Kumar, Ganesh Bhattarai and Dipendra Karki (Mar. 2021). "Management Accounting Practices on Organizational Performance Mediated by Rationalized Managerial Decisions." In: *International Research Journal of Management Science* 5.1, pp. 148–167. ISSN: 2542-2510. 10.3126/irjms.v5i1.35870. http://dx.doi.org/10.3126/irjms.v5i1.35870.

Dhital, Hemant (2025). "The evolving landscape of Cybercrime in Nepal: A multi-Year Analysis of Platform Specific Trends and Victim Demographics (2077-2082 B.S. / 2020-2025 A.D.)" In: *Applied Data Science and Analysis* 2025, pp. 165–177. ISSN: 3005-317X. 10.58496/adsa/2025/014. http://dx.doi.org/10.58496/ADSA/2025/014.

Financial Intelligence Unit, Nepal Rastra Bank (2024). *Strategic Analysis Report 2024: Cyber Enabled Frauds*. Tech. rep. Kathmandu: Nepal Rastra Bank. https://www.nrb.org.np/contents/uploads/2024/11/FIU-Nepal-Strategic-Analysis-Report-2024.pdf.pdf.

Gartner (2026). *AI Maturity Model and AI Roadmap Toolkit*. Online. Accessed 28 June 2026. https://www.gartner.com/en/chief-information-officer/research/ai-maturity-model-toolkit.

Gupta, Lokesh (2024). "Issues of Cyber security and its solutions in Nepalese Context." In: *NPRC Journal of Multidisciplinary Research* 1.2, pp. 122–127. ISSN: 3059-9148. 10.3126/nprcjmr.v1i2.69333. http://dx.doi.org/10.3126/nprcjmr.v1i2.69333.

Hernandez Aros, Ludivia, Luisa Ximena Bustamante Molano, Fernando Gutierrez-Portela, John Johver Moreno Hernandez and Mario Samuel Rodríguez Barrero (2024). "Financial fraud detection through the application of machine learning techniques: a literature review." In: *Humanities and Social Sciences Communications* 11.1. ISSN: 2662-9992. 10.1057/s41599-024-03606-0. http://dx.doi.org/10.1057/s41599-024-03606-0.

Hilal, Waleed, S. Andrew Gadsden and John Yawney (May 2022). "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances." In: *Expert Systems with Applications* 193, p. 116429. ISSN: 0957-4174. 10.1016/j.eswa.2021.116429. http://dx.doi.org/10.1016/j.eswa.2021.116429.

Irianto, Aloysius Bagas Pradipta and Pisit Chanvarasuth (May 2025). "Drivers and Barriers of Mobile Payment Adoption Among MSMEs: Insights from Indonesia." In: *Journal of Risk and Financial Management* 18.5, p. 251. ISSN: 1911-8074. 10.3390/jrfm18050251. http://dx.doi.org/10.3390/jrfm18050251.

J. Skulmoski, Gregory, Francis T. Hartman and Jennifer Krahn (2007). "The Delphi Method for Graduate Research." In: *Journal of Information Technology Education: Research* 6, pp. 001–021. ISSN: 1539-3585. 10.28945/199. http://dx.doi.org/10.28945/199.

Karki, Dipendra (2012). *Economic impact of tourism in Nepal's economy using cointegration and error correction model*. en. 10.13140/RG.2.1.4839.5684. https://www.researchgate.net/doi/10.13140/RG.2.1.4839.5684.

Klapper, Leora, Dorothe Singer, Laura Starita and Alexandra Norris (2025). *The Global Findex Database 2025: Connectivity and Financial Inclusion in the Digital Economy*. Washington, DC: World Bank. ISBN: 9781464822049. 10.1596/978-1-4648-2204-9. http://dx.doi.org/10.1596/978-1-4648-2204-9.

Manzini, Dumisani, Rudolph Oosthuizen, Hilda Chikwanda and Rina Peach (Apr. 2026). "SystemsBased Organisational Resilience Framework: A Delphi StudyBased Validation and Verification." In: *Systems Research and Behavioral Science* 43.4, pp. 1615–1644. ISSN: 1099-1743. 10.1002/sres.70061. http://dx.doi.org/10.1002/sres.70061.

MIT Sloan Management Review (2026). *What's Your Company's AI Maturity Level?* Online. Accessed 28 June 2026. https://mitsloan.mit.edu/ideas-made-to-matter/whats-your-companys-ai-maturity-level.

Nepal News (2026). *Everything You Need to Know about NRB's New Regulatory Sandbox*. Online. Accessed 28 June 2026. https://english.nepalnews.com/s/business/everything-you-need-to-know-about-nrbs-new-regulatory-sandbox/.

Nepal Rastra Bank (2024). *Annual Report Fiscal Year 2023/24*. Tech. rep. Kathmandu: Nepal Rastra Bank. https://www.nrb.org.np/contents/uploads/2025/07/Annual-Report-2023-24-English.pdf.

Nicholls, Jack, Aditya Kuppa and Nhien-An Le-Khac (2021). "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape." In: *IEEE Access* 9, pp. 163965–163986. ISSN: 2169-3536. 10.1109/access.2021.3134076. http://dx.doi.org/10.1109/ACCESS.2021.3134076.

Pathak, Arbind (Feb. 2024). "Digital Payment In Nepal: An Overview And Recommendations." In: *Rupandehi Campus Journal* 4.1, pp. 25–34. ISSN: 2976-1158. 10.3126/rcj.v4i1.62916. http://dx.doi.org/10.3126/rcj.v4i1.62916.

Rubio, Jeniffer and Ana Belén Tulcanaza-Prieto (May 2025). "Digital Payments Trust in Latin America and the Caribbean." In: *Economies* 13.5, p. 140. ISSN: 2227-7099. 10.3390/economies13050140.

Tamang, Abinash, Prem Kumar Bhaskar and Jyotir Moy Chatterjee (2021). "Acceleration of Digital Payment Adoption during COVID-19 Pandemic: A Case Study of Nepal." In: *LBEF Research Journal of Science, Technology and Management* 3.2, pp. 1–13.

The Kathmandu Post (Dec. 2025a). *Nepal Rastra Bank Drafts AI Guideline for Banks and Digital Payment Firms*. Online. Accessed 28 June 2026. https://kathmandupost.com/money/2025/12/12/nepal-rastra-bank-drafts-ai-guideline-for-banks-and-digital-payment-firms.

– (Mar. 2025b). *Nepal's Central Bank Amends Online Payment System Directives to Curb Fraud*. Online. Accessed 28 June 2026. https://kathmandupost.com/money/2025/03/07/nepal-s-central-bank-amends-online-payment-system-directives-to-curb-fraud.

Torraco, Richard J. (Oct. 2016). "Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future." In: *Human Resource Development Review* 15.4, pp. 404–428. ISSN: 1552-6712. 10.1177/1534484316671606. http://dx.doi.org/10.1177/1534484316671606.

Vanini, Paolo, Sebastiano Rossi, Ermin Zvizdic and Thomas Domenig (Mar. 2023). "Online payment fraud: from anomaly detection to risk management." In: *Financial Innovation* 9.1. ISSN: 2199-4730. 10.1186/s40854-023-00470-w. http://dx.doi.org/10.1186/s40854-023-00470-w.

Whittemore, Robin and Kathleen Knafl (Nov. 2005). "The integrative review: updated methodology." In: *Journal of Advanced Nursing* 52.5, pp. 546–553. ISSN: 1365-2648. 10.1111/j.1365-2648.2005.03621.x. http://dx.doi.org/10.1111/j.1365-2648.2005.03621.x.

Widayani, Anna, Nilawati Fiernaningsih and Pudji Herijanto (Dec. 2022). "Barriers to digital payment adoption: micro, small and medium enterprises." In: *Management & Marketing* 17.4, pp. 528–542. ISSN: 2069-8887. 10.2478/mmcks-2022-0029. http://dx.doi.org/10.2478/mmcks-2022-0029.