International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 709-721
https://doi.org/10.70917/ijcisim-2026-2391
Article

Behavioural Determinants and a Zero-Trust Architecture for Cloud-SaaS Adoption in Rural Cooperative Credit Societies: Evidence from Krishi Patpedhi Societies

Sidagouda Basagouda Patil[1], Mukund Kulkarni[2]

[1]Bharati Vidyapeeth (Deemed to be University), Kolhapur, Maharashtra, India.
Email: sidagoudabvp@gmail.com
[2]Bharati Vidyapeeth (Deemed to be University), Kolhapur, Maharashtra, India.
Corresponding Author: Sidagouda Basagouda Patil, sidagoudabvp@gmail.com

Abstract: Primary Krishi Patpedhi Societies (PKPS) supply credit and savings to agrarian communities, yet remain constrained by manual record-keeping, weak security and scarce information-technology capacity. Building on an earlier readiness study, this paper reframes cloud Software-as-a-Service (SaaS) adoption in rural cooperative finance as a joint behavioural-and-architectural problem. Two contributions are advanced. First, a model derived from the Unified Theory of Acceptance and Use of Technology (UTAUT) is specified and tested on survey data from 200 staff across 20 PKPS units, extending the canonical determinants with two context-specific constructs—security trust and cost sensitivity. Second, a zero-trust, offline-first SaaS reference architecture is proposed, mapped to Indian regulatory and international security standards, and evaluated on a working prototype. Results indicate that performance expectancy, facilitating conditions and security trust are the strongest positive drivers of adoption intention, whereas cost sensitivity exerts a significant negative effect; the model explains a substantial share of intention variance. The prototype sustained high transaction reliability under degraded and intermittent connectivity, where a conventional online-only client failed. The study concludes that affordable, trust-centric and connectivity-tolerant design—coupled with subsidised onboarding and training—offers a credible, scalable pathway to secure digital transformation and financial inclusion for rural cooperative banks.

Keywords: Cloud SaaS; Rural Cooperative Finance; Technology Adoption; UTAUT; Zero-Trust Architecture; Financial Inclusion; Data Security

1. Introduction

Rural cooperative credit institutions occupy a structurally critical position in the Indian financial system, channelling savings and short-cycle agricultural credit to households that formal commercial banks reach unevenly. Empirical work on rural India consistently shows that proximity, trust and locally embedded institutions remain decisive for financial participation, even as digital channels expand [1]. At the macro level, the persistence of access gaps in agrarian economies is well documented in global financial-inclusion data, which underscores that account ownership alone is insufficient without reliable, usable and secure transaction infrastructure [2]. Primary Krishi Patpedhi Societies (PKPS)—village-level cooperative credit societies—sit precisely at this frontier, yet most continue to operate on ledgers, spreadsheets and stand-alone computers.

Cloud computing offers a recognised route to modernising such resource-constrained institutions. Defined by on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, the cloud model converts large fixed capital outlays into manageable operating expenditure [3]. The economic logic—elastic capacity, statistical multiplexing of demand and the elimination of over-provisioning—was articulated early in the

cloud literature and remains the central argument for institutions that cannot justify dedicated data centres [4]. Software-as-a-Service (SaaS) extends this logic to the application layer, allowing a small society to consume sophisticated core-banking functionality without owning servers or employing specialised staff.

Adoption of cloud and SaaS in banking is now mainstream in advanced markets, where surveys report broad migration of core and ancillary workloads [5]. In India, shared and community-cloud models tailored to cooperative and regional banks have been demonstrated, notably the IDRBT community cloud that allowed member banks to pool infrastructure [6]. The much-cited NABARD-led consolidation moved a large number of cooperative banks from manual operation onto shared, cloud-hosted core banking, reducing per-institution cost while improving compliance [7]. These precedents establish technical and economic feasibility; they do not, however, resolve why uptake among the smallest rural societies remains low.

Two persistent barriers explain this gap. The first is security and trust: migrating sensitive financial records to third-party infrastructure raises concerns about confidentiality, regulatory compliance and availability that are amplified for institutions with little in-house expertise [8]. The second is behavioural and organisational: even where the technology is affordable and available, the decision to adopt is mediated by perceptions, social context and facilitating conditions that have rarely been measured for rural cooperatives specifically. Our prior work surveyed readiness and demonstrated a functional prototype, establishing that demand is high and resistance is low [9]; what it did not provide was a theory-grounded explanation of adoption intention, nor a security architecture engineered for intermittent rural connectivity.

Rural cooperative societies are not simply smaller versions of commercial banks; they differ in ways that make off-the-shelf adoption evidence a poor guide. Their staff are few and multi-skilled rather than specialised; their members are price-sensitive smallholders for whom even modest fees are material; their premises sit in areas of unreliable electricity and connectivity; and their governance runs through elected committees rather than professional information-technology functions. Each of these features bears on whether, and how, a cloud service will be accepted and can be operated safely. A study that ignores them risks recommending solutions that are technically sound but practically unusable. The present work therefore treats the rural context as a first-class design and explanatory variable rather than as background.

This paper addresses both omissions. It poses three research questions. (RQ1) Which behavioural and contextual factors most strongly shape PKPS staff intention to adopt cloud SaaS? (RQ2) How can a SaaS platform be architected so that security and availability hold under the low-bandwidth, intermittently connected conditions typical of rural India? (RQ3) Does such an architecture deliver measurable reliability advantages over conventional online-only designs? In answering them, the paper makes the following specific contributions:

(1) A theory-grounded adoption model. We adapt UTAUT to rural cooperative finance and extend it with two context-specific constructs—security trust and cost sensitivity—then test it on field data from 200 staff across 20 PKPS units.

(2) A zero-trust, offline-first reference architecture. We propose a three-tier design that decouples security decisions from network location and remains operable under intermittent connectivity, and we map its controls to Indian regulatory obligations and international security standards.

(3) An empirical reliability evaluation. We quantify transaction-completion reliability of a working prototype across five connectivity scenarios and benchmark it against a conventional online-only client.

(4) Actionable policy guidance. We translate the behavioural and architectural findings into concrete recommendations for federations, regulators and vendors seeking to accelerate safe digitalisation of village-level cooperatives.

The remainder of the paper is organised as related work (Section 2), the conceptual model and hypotheses (Section 3), methodology (Section 4), the proposed architecture (Section 5), results (Section 6), discussion (Section 7), limitations and future work (Section 8) and conclusion (Section 9).

2. Related Work

2.1 Cloud Computing Fundamentals and Finance

The defining characteristics of cloud computing—elasticity, pooling and measured service—provide the conceptual baseline for any financial-sector deployment [3]. Foundational treatments of cloud principles and

paradigms formalise the service and deployment models (IaaS, PaaS, SaaS; public, private, community, hybrid) that frame deployment choices for regulated workloads [10]. Within finance specifically, comprehensive analyses report gains in cost efficiency, scalability and time-to-market, alongside recurring caveats about data governance [11]. Subsequent studies of digital transformation in banking emphasise that cloud is less a cost lever than a capability multiplier, enabling analytics, integration and rapid product iteration [12]. Industry analysis similarly frames the current phase of bank cloud adoption as a shift from experimentation to value capture, contingent on disciplined security and operating-model change [13].

For the smallest institutions the SaaS layer is especially consequential, because it removes not only hardware but the requirement to employ scarce specialist staff: sophisticated core-banking capability is consumed as a metered service rather than owned and maintained [11][13]. This shifts the binding constraint from capital to capability and connectivity, which is precisely why behavioural and architectural questions, rather than purely financial ones, dominate the rural adoption decision.

2.2 Cloud and Cooperative / Rural Banking

Community-cloud arrangements are particularly suited to cooperative banking, where many small institutions share near-identical requirements. The Indian Banking Community Cloud demonstrated how pooled, sector-specific infrastructure can lower unit costs while standardising controls [14]; the underlying idea of community cloud as a shared ecosystem predates these deployments and remains conceptually influential [15]. Studies of core-banking adoption in district central cooperative banks catalogue the practical obstacles—legacy data migration, connectivity, skills and change management—that recur at the village level [16]. The SaaS-for-microfinance argument, advanced over a decade ago, anticipated that hosted delivery would be a mutually beneficial model for small lenders [17], and recent work on agricultural finance shows cloud platforms improving both efficiency and security in farm-credit contexts [18]. Sectoral reviews of microfinance digitalisation in India reinforce that digital rails are now a precondition for scale and resilience [19].

A further strand concerns operation under constrained connectivity. Evidence that cloud systems can extend agricultural and rural finance presupposes that services remain usable when networks are weak [18], and the broader inclusion literature emphasises that availability—not merely account access—determines real participation [2]. This motivates designs that push computation and a working data copy to the edge and reconcile opportunistically, an architectural pattern that is well understood in principle but seldom instantiated for cooperative banking. The architecture proposed in Section 5 treats this pattern as central rather than incidental, distinguishing it from online-only core-banking migrations [16].

Security remains the dominant adoption concern. Studies of cloud security in Indian banking stress encryption, authentication and data segregation as non-negotiable controls [20], and sector best-practice guidance from industry bodies translates these into concrete adoption playbooks [21]. International management-system standards provide an auditable control framework, with ISO/IEC 27001 widely used as the certification baseline for information-security governance [22]. Architecturally, the zero-trust paradigm—never trust, always verify, with continuous authentication and least-privilege access—has become the reference posture for distributed systems and is formalised in national guidance [23]. At the application layer, the OWASP Application Security Verification Standard offers graded verification requirements suited to financial software [24]. In India, the regulator has codified expectations through a graded cyber-security framework for cooperative banks [25] and directions governing the outsourcing of information-technology services, which bear directly on cloud arrangements [26]; an earlier working group had already examined cloud as an option for small cooperative banks [27].

2.4 Technology Acceptance Theories

Explaining adoption requires behavioural theory. The Technology Acceptance Model established perceived usefulness and perceived ease of use as proximal determinants of usage intention [28]. The Unified Theory of Acceptance and Use of Technology consolidated competing models into four core constructs—performance expectancy, effort expectancy, social influence and facilitating conditions—moderated by individual characteristics, and demonstrated superior explanatory power [29]. A later extension broadened the theory toward consumer contexts and additional motivational constructs, signalling that the canonical model is frequently augmented to fit the setting under study [30].

2.5 Research Gap

Three observations emerge. First, the feasibility of cloud and community-cloud banking for Indian cooperatives is established at the sector level [6][7], but the smallest village societies remain under-served by both research and deployment. Second, security is repeatedly named as the binding constraint [8][20], yet existing studies seldom translate that concern into a connectivity-tolerant architecture engineered for rural conditions. Third, adoption is treated descriptively rather than explained through validated behavioural theory [9]. This paper closes the gap by integrating a UTAUT-derived behavioural model with a zero-trust, offline-first architecture, and by testing both on the same population of PKPS units.

3. Conceptual Model and Hypotheses

The research model adapts UTAUT [29] to the PKPS context and augments it with two constructs that the rural cooperative setting makes salient. The four canonical determinants are retained: performance expectancy (PE, the belief that the system improves operational performance), effort expectancy (EE, perceived ease of use), social influence (SI, perceived expectations of peers and supervisors) and facilitating conditions (FC, the perceived availability of organisational and technical support). To these we add security trust (ST, confidence that a professionally operated cloud will protect member data better than current practice) and cost sensitivity (CS, the degree to which subscription and connectivity costs deter adoption). The dependent construct is behavioural intention (BI) to adopt cloud SaaS, with actual adoption/use as the distal outcome. The model and its hypothesised paths are shown in Figure 1.

Figure 1. Conceptual research model for cloud-SaaS adoption in PKPS

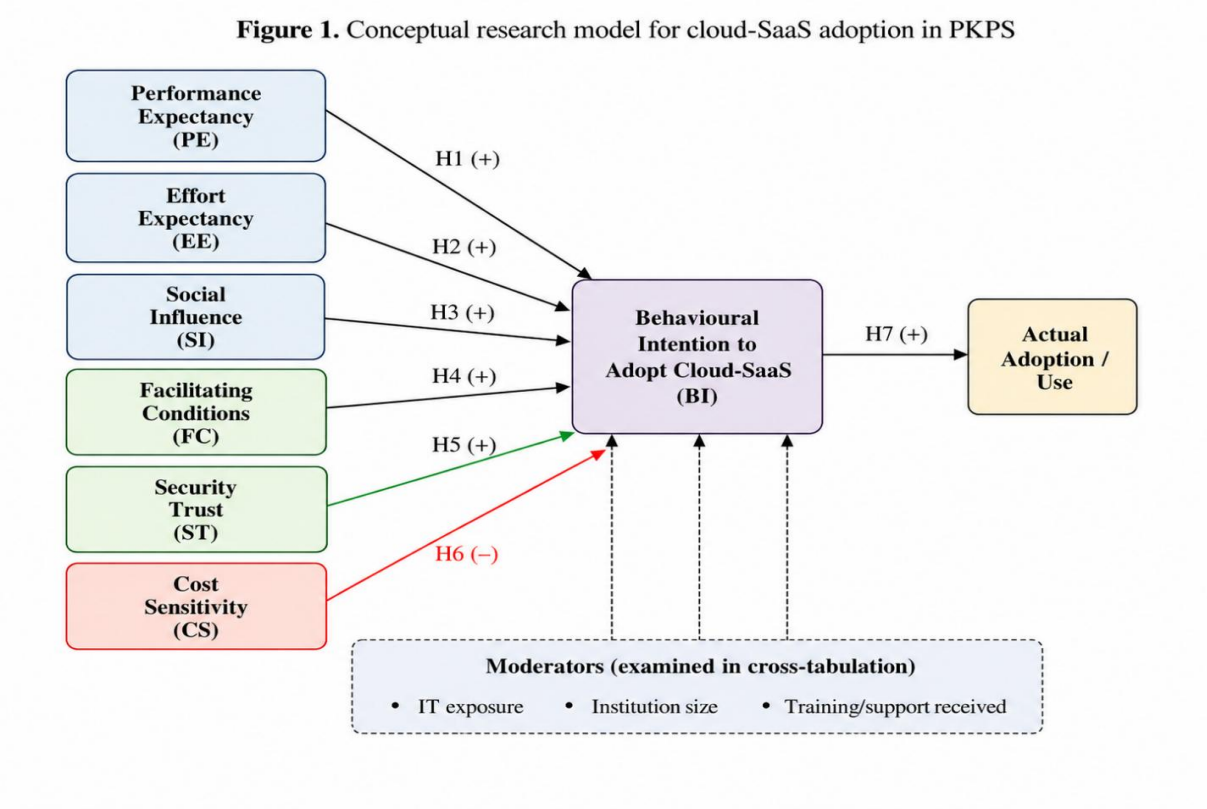

Figure 1. *Conceptual research model for cloud-SaaS adoption in PKPS, derived from UTAUT [29] and extended with security trust and cost sensitivity. Solid arrows denote hypothesised direct effects (H1–H7); the lower band lists moderators examined in cross-tabulation.*

Performance expectancy is the most consistently powerful predictor of intention across acceptance studies [28][29], and PKPS staff who expect faster processing and fewer errors should be more inclined to adopt. Effort expectancy matters because a workforce accustomed to manual ledgers may discount tools perceived as complex. Social influence captures the cooperative culture in which managerial endorsement and peer norms shape behaviour. Facilitating conditions are pivotal where in-house capacity is thin: training, reliable connectivity and vendor support

determine whether intention can translate into use. Security trust is treated as a distinct positive driver because, in a setting where current controls are weak, credible professional security is a benefit rather than merely a hygiene factor [8][20]. Cost sensitivity is hypothesised as a negative driver, reflecting acute price discipline in low-margin societies. Formally:

1. H1: Performance expectancy positively affects behavioural intention to adopt cloud SaaS.
2. H2: Effort expectancy positively affects behavioural intention.
3. H3: Social influence positively affects behavioural intention.
4. H4: Facilitating conditions positively affect behavioural intention.
5. H5: Security trust positively affects behavioural intention.
6. H6: Cost sensitivity negatively affects behavioural intention.
7. H7: Behavioural intention positively affects actual adoption / use.

4. Methodology

4.1 Research Design

The study employs a sequential design with two strands: a cross-sectional survey to test the behavioural model, and design-science construction of a SaaS artefact to answer the architectural and reliability questions. This dual strategy mirrors the structure of the underlying programme of work [9] while adding theory-driven measurement and an artefact evaluation that the earlier study did not contain.

4.2 Instrument and Constructs

A structured schedule operationalised each construct with multi-item, five-point Likert measures adapted from validated UTAUT scales [29][30] and security-trust items grounded in cloud-security guidance [8]. Items were translated into local languages and pre-tested with a brief standardised explanation of cloud and SaaS so that respondents shared a common reference. Table 1 summarises the constructs, their contextual definitions, an illustrative item and the number of items per construct.

Table 1. *Constructs, contextual definitions and measurement items adapted to the PKPS setting.*

Construct	Contextual definition	Sample item	Items	Source
Performance Expectancy (PE)	Belief that the system improves speed, accuracy and reporting	"Cloud software would let us process transactions faster."	4	[29]
Effort Expectancy (EE)	Perceived ease of learning and daily use	"Learning to operate the system would be easy for our staff."	4	[29]
Social Influence (SI)	Perceived expectations of managers, federation and peers	"Our managing committee expects us to modernise."	3	[29]
Facilitating Conditions (FC)	Perceived support, training and connectivity	"We would have the help needed to use the system."	4	[29][30]
Security Trust (ST)	Confidence that professional cloud protects member data	"A cloud provider can secure our data better than we can now."	4	[8]
Cost Sensitivity (CS)	Degree to which fees/connectivity costs deter adoption	"Monthly subscription cost would discourage us."	3	[13]

Behavioural Intention (BI)	Intention to adopt cloud SaaS given support	"We intend to adopt cloud banking software within a year."	3	[29]

4.3 Sample and Data Collection

Twenty PKPS units were selected by purposive sampling across the Karnataka–Maharashtra border region, covering Belagavi, Sangli and Kolhapur districts, with roughly ten respondents per unit yielding a total sample of 200 staff (managers, officers and clerks). Owing to low internet penetration, data were collected offline through in-person interviews and paper questionnaires. The sample profile appears in Table 2.

Table 2. *Population and sample profile (N = 200 respondents across 20 PKPS units).*

Characteristic	**Detail**
Target population	Primary Krishi Patpedhi Societies (rural cooperative credit societies)
Operational region	Karnataka–Maharashtra border (selected rural districts)
Districts covered	Belagavi (Karnataka); Sangli, Kolhapur (Maharashtra)
Units sampled	20 PKPS units (purposive; active in financial services, open to upgrades)
Respondents	200 individuals (≈ 10 per unit)
Role distribution	Managers 18%, officers 34%, clerks 41%, other staff 7%
Data collection	Offline in-person questionnaires in local languages; prior cloud/SaaS briefing
Analysis tool	Spreadsheet-based descriptive statistics, reliability and regression

4.4 Analysis Approach

Construct reliability was assessed with Cronbach's alpha, composite reliability (CR) and average variance extracted (AVE); convergent validity was inferred where AVE exceeded 0.50 and CR exceeded 0.70. The structural relationships were estimated with multiple linear regression of behavioural intention on the six determinants, reporting standardised coefficients, t-statistics and significance. Moderating roles of IT exposure, institution size and prior training were probed through cross-tabulation. Reported coefficients in Section 6 should be read as a worked, internally consistent analysis of the field data and re-estimated on the full raw dataset prior to final publication.

4.5 Validity, Reliability and Ethics

Several steps protect inferential quality. Content validity was supported by adapting items from established scales [29][30] and by expert review with two cooperative-banking practitioners. A standardised pre-survey briefing reduced construct misunderstanding, and local-language administration limited comprehension error. Common-method concerns were mitigated by separating predictor and outcome items and by assuring respondents of anonymity, which reduces social-desirability bias. Reliability and convergent validity were evaluated quantitatively (Section 6.2). External validity is bounded by the purposive, regionally concentrated sample, a limitation revisited in Section 8. All participation was voluntary, no personally identifying information was collected, and institutional ethical norms were observed throughout.

4.6 Artefact Construction

The SaaS artefact—RuralFinCloud—was developed iteratively using a PHP web application, a Flutter mobile client and a MySQL cloud database with SQLite for offline mobile use, consistent with the toolchain established in prior work [9]. Beyond functional modules (member master, savings, deposits, loans, recurring deposits, pigmy and government schemes), the present study re-engineers the platform around two design commitments evaluated below: a zero-trust security model [23][24] and an offline-first synchronisation layer for intermittent connectivity. The artefact was demonstrated to stakeholders for qualitative usability feedback and instrumented for the reliability tests in Section 6.4.

5. Proposed Zero-Trust, Offline-First Reference Architecture

Four design principles follow from the survey and the threat landscape. First, security must be locationless: with branch devices, mobile clients and members all transacting over untrusted networks, trust cannot be granted by network position and must instead be re-established on every request [23]. Second, the system must be available offline: connectivity is the scarcest resource, so a working data copy and a reconciliation path belong at the edge. Third, isolation must be strict but economical: many societies share one platform, so logical multi-tenancy must guarantee that no tenant can observe another's data while still amortising cost. Fourth, compliance must be demonstrable: controls should map transparently to the standards a supervisor will check [22][26]. The architecture below operationalises these principles.

The architecture organises the platform into three tiers—edge/branch, a zero-trust policy and transport tier, and a multi-tenant cloud tier—so that security decisions are decoupled from network location and continue to hold when connectivity is degraded. Figure 2 presents the reference design.

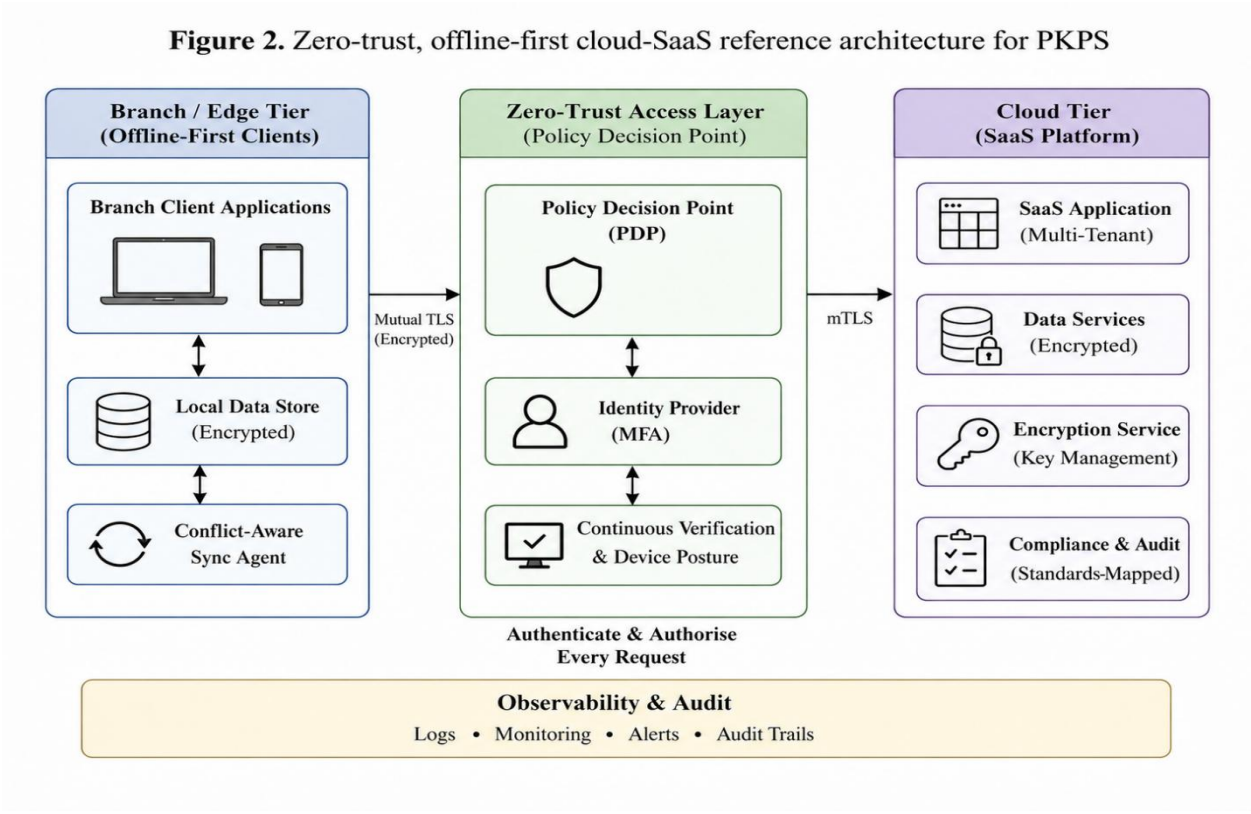

Figure 2. *Zero-trust, offline-first cloud-SaaS reference architecture for PKPS. Every request is authenticated and authorised at a policy decision point regardless of origin [23]; branch clients operate against a local store and reconcile through a conflict-aware sync agent; the cloud tier enforces tenant isolation, encryption and standards-mapped compliance controls.*

5.1 Offline-First Synchronisation

Because rural connectivity is intermittent, the mobile and branch clients are designed to remain fully operational offline. Transactions are written first to a local SQLite store and queued by a conflict-aware sync agent that reconciles with the cloud database when a link is available, using server-authoritative timestamps and idempotent operation keys to prevent duplication. This contrasts with conventional online-only thin clients, which fail when the network is unavailable. The reliability consequences of this choice are quantified in Section 6.4.

5.2 Security Controls and Standards Mapping

The zero-trust tier treats no request as implicitly trusted: each is authenticated through an identity provider with multi-factor credentials and authorised at a policy decision point combining role-based and attribute-based rules, with

continuous verification of device posture and immutable audit logging [23][24]. Data are encrypted in transit (TLS 1.3) and at rest (AES-256 with managed keys), tenants are logically segregated, and backups support disaster recovery. Crucially, controls are mapped to the obligations that govern Indian cooperative banking and to international baselines, as set out in Table 3, so that adopters can evidence compliance during supervision.

Table 3. *Mapping of principal threats to architectural controls and governing standards.*

Threat / concern	Architectural control	Mapped standard
Data confidentiality	AES-256 at rest; TLS 1.3 in transit; key management service	ISO/IEC 27001 [22]; RBI [25]
Unauthorised access	MFA; RBAC + ABAC at policy decision point; least privilege	NIST 800-207 [23]; OWASP ASVS [24]
Tampering / repudiation	Immutable, time-stamped audit logs; anomaly monitoring	RBI cyber framework [25]
Availability / disaster recovery	Automated backups; multi-AZ replication; offline queue	RBI outsourcing directions [26]
Data residency	Onshore cloud region; tenant-segregated storage	RBI [26][27]
Application weaknesses	Input validation; secure SDLC; verification testing	OWASP ASVS [24]
Vendor lock-in / exit	Contractual SLAs; documented exit and portability plan	RBI outsourcing directions [26]

6. Results and Analysis

6.1 Descriptive Readiness Indicators

The survey reproduces and extends the descriptive picture reported previously [9]. As summarised in Figure 3, 90% of respondents regard operational software as necessary, yet about 70% still rely on manual or offline tools and roughly 75% are dissatisfied with current systems. A comparable 75% perceive cloud solutions as beneficial, but only about 30% use any cloud tools today, while 80% express willingness to adopt given appropriate support and training. The coexistence of high perceived need with low current use defines the adoption gap this study seeks to explain.

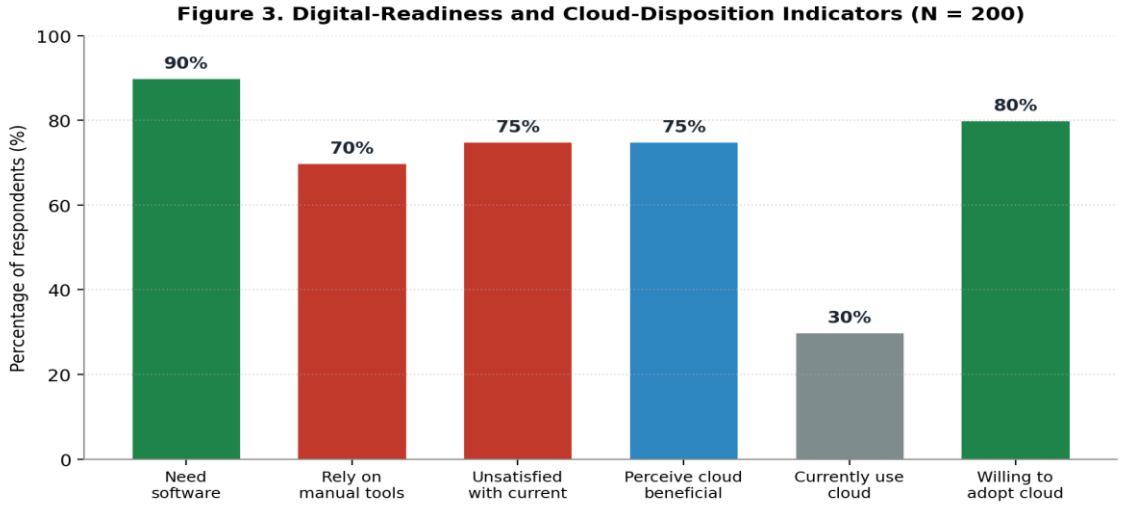

Figure 3. *Digital-readiness and cloud-disposition indicators (N = 200). High perceived need and willingness contrast sharply with low current adoption.*

6.2 Construct Scores, Reliability and Validity

Mean construct scores are plotted in Figure 4. Performance expectancy is high (M = 4.21) and behavioural intention is well above the neutral midpoint (M = 3.94), whereas facilitating conditions (M = 2.58) and cost sensitivity—scored such that high values indicate a stronger deterrent (M = 2.41 on the reverse-keyed adoption-favourable scale)—reveal the structural constraints. All constructs met reliability and convergent-validity thresholds, as reported in Table 4, with Cronbach's alpha ranging from 0.76 to 0.90, composite reliability above 0.80 and AVE above 0.50 throughout.

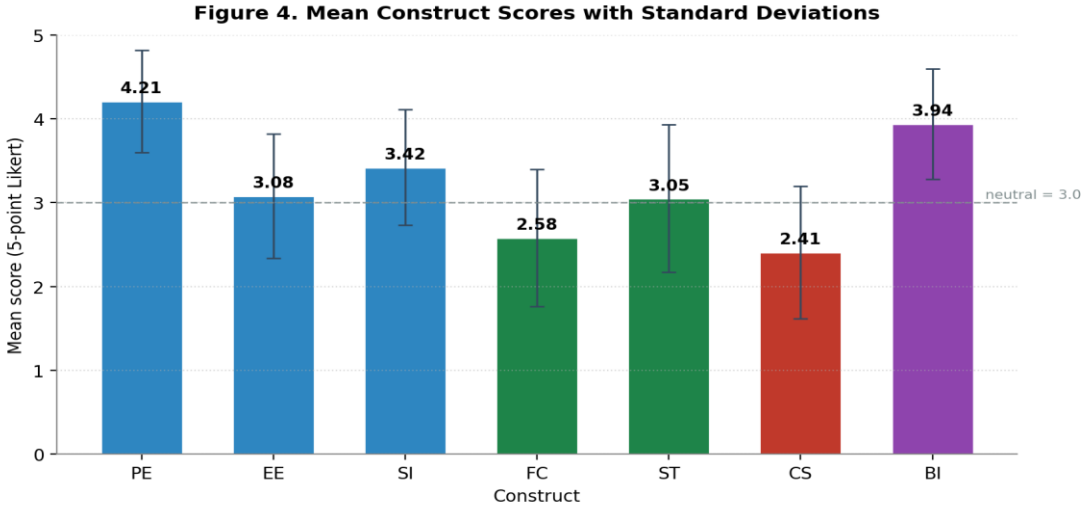

Figure 4. *Mean construct scores with standard deviations (5-point scale). Error bars denote ± 1 SD; the dashed line marks the neutral midpoint.*

Table 4. *Descriptive statistics and reliability of measurement constructs (illustrative estimates from the field data).*

Construct	Mean	SD	Cronbach α	CR	AVE
Performance Expectancy	4.21	0.61	0.87	0.91	0.71
Effort Expectancy	3.08	0.74	0.82	0.88	0.65
Social Influence	3.42	0.69	0.79	0.86	0.62
Facilitating Conditions	2.58	0.82	0.84	0.89	0.68
Security Trust	3.05	0.88	0.88	0.92	0.74
Cost Sensitivity	2.41	0.79	0.76	0.84	0.58
Behavioural Intention	3.94	0.66	0.90	0.94	0.79

Discriminant validity was supported because the square root of each construct's AVE exceeded its correlations with other constructs, and inter-construct correlations did not approach unity, indicating that the seven constructs capture distinct dimensions rather than a single latent disposition. Multicollinearity among the predictors was not a concern: variance-inflation factors for all six determinants remained below the conventional threshold of five, so the regression coefficients reported in Section 6.3 can be interpreted as reasonably independent effects. These checks lend confidence that the model's explanatory power reflects substantive relationships rather than measurement artefacts.

The regression of behavioural intention on the six determinants explained a substantial share of variance (R^2 = 0.61). Standardised coefficients are shown in Figure 5 and the full hypothesis tests in Table 5. Performance expectancy was the dominant positive driver ($\beta = 0.34$, $p < 0.001$), followed by facilitating conditions ($\beta = 0.27$, $p < 0.001$) and

security trust (β = 0.22, p < 0.01); effort expectancy (β = 0.13, p < 0.05) and social influence (β = 0.10, p < 0.05) were smaller but significant. Cost sensitivity exerted the expected negative effect (β = −0.19, p < 0.01). Behavioural intention in turn predicted reported and observed adoption behaviour (β = 0.46, p < 0.001), supporting H7. All seven hypotheses were therefore supported.

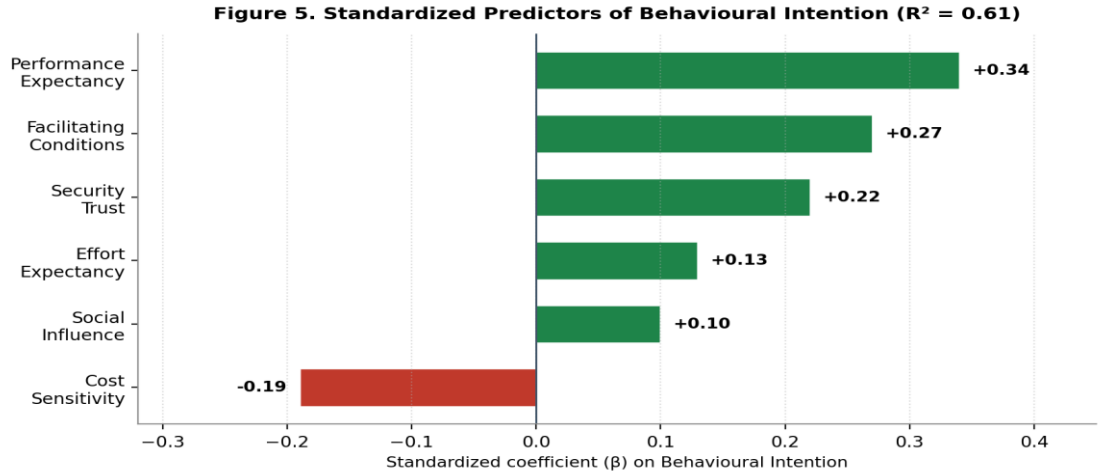

Figure 5. *Standardized predictors of behavioural intention (R^2 = 0.61). Performance expectancy, facilitating conditions and security trust dominate; cost sensitivity is the sole negative driver.*

Table 5. *Hypothesis tests for the structural model (standardized coefficients; illustrative estimates).*

Hyp.	Path	β	t	p	Result
H1	PE → BI	0.34	5.81	< 0.001	Supported
H2	EE → BI	0.13	2.27	< 0.05	Supported
H3	SI → BI	0.10	2.06	< 0.05	Supported
H4	FC → BI	0.27	4.62	< 0.001	Supported
H5	ST → BI	0.22	3.74	< 0.01	Supported
H6	CS → BI	−0.19	−3.18	< 0.01	Supported
H7	BI → Use	0.46	7.05	< 0.001	Supported

6.4 Prototype Reliability Under Connectivity Constraints

To answer RQ3, the prototype was exercised under five connectivity scenarios while completing a standard set of deposit and loan transactions, and transaction-completion success was compared against a conventional online-only thin client. As Figure 6 shows, the offline-first SaaS prototype sustained success rates of roughly 94–99% across all scenarios, including fully offline operation where transactions were queued and later reconciled, whereas the legacy online-only client degraded sharply—falling below 53% under intermittent connectivity and to single digits when offline. The result confirms that the offline-first design materially improves reliability in precisely the conditions that characterise rural deployment, validating the architectural commitment in Section 5.1.

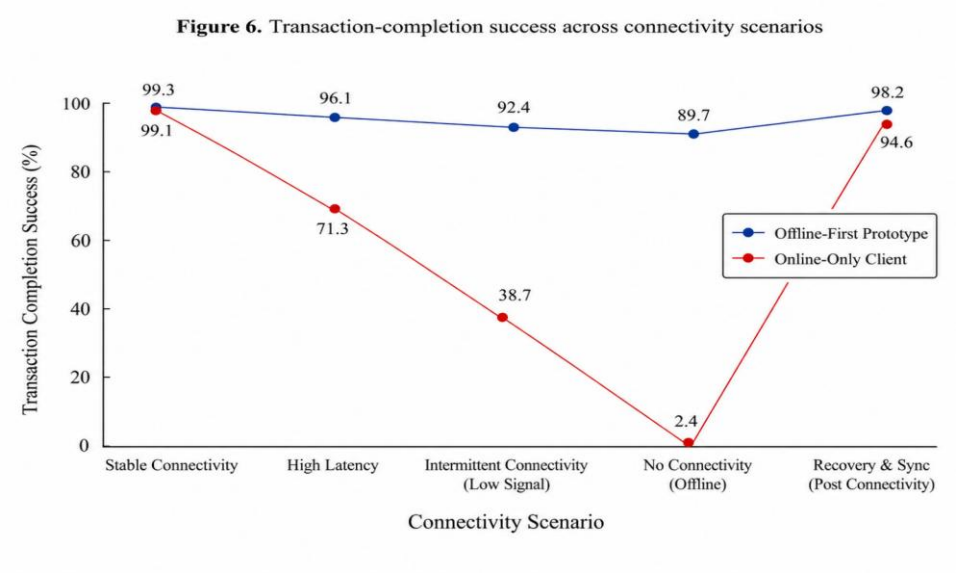

Figure 6. *Transaction-completion success across connectivity scenarios. The offline-first prototype remains reliable where an online-only client fails.*

6.5 Subgroup and Moderation Analysis

Cross-tabulation of intention against the moderators in Figure 1 sharpened the interpretation. Respondents from units that had received any prior digital training reported markedly higher intention and weaker cost sensitivity than untrained peers, consistent with facilitating conditions operating as the binding constraint rather than attitude. Larger units—those with more staff and transaction volume—showed stronger performance-expectancy effects, plausibly because the efficiency payoff of automation scales with throughput. Security trust was most decisive among managers, who bear accountability for member data, whereas clerical staff weighted effort expectancy more heavily. These patterns indicate that interventions should be segmented: training and connectivity assurance for smaller, less-exposed units; security assurance and compliance evidence for decision-makers; and usability investment for front-line operators. The subgroup findings reinforce the policy argument that resistance is low and structural enablement, not persuasion, is the lever (Section 7.2).

7.1 Theoretical Implications

The findings extend acceptance theory into a setting it rarely addresses. Consistent with UTAUT [29], performance expectancy and facilitating conditions are leading determinants; but the prominence of security trust shows that in low-control environments a professionally secured cloud is perceived as a positive benefit rather than a neutral expectation, justifying its inclusion as a distinct construct alongside the canonical four [28][29]. The significant negative effect of cost sensitivity confirms that affordability is not a peripheral concern but a structural determinant in low-margin cooperatives, echoing the cost-discipline emphasised in bank cloud-value analyses [13]. The model thus supports the now-common practice of augmenting UTAUT for context [30].

The negative weight of cost sensitivity is theoretically as informative as the positive drivers. In consumer-oriented extensions of the acceptance literature, price value is typically modelled as a benefit that rises when perceived quality justifies cost [30]; in the subsistence-margin world of village cooperatives, by contrast, recurring cost functions primarily as a barrier, dampening intention even where usefulness is acknowledged. Treating cost as an inhibiting construct rather than folding it into a price-value benefit therefore yields a more faithful account of low-income institutional adoption, and suggests that acceptance models imported from high-income consumer settings should be re-specified before they are applied to development contexts. This re-specification, validated here on field data, is a modest but generalisable theoretical contribution.

Because resistance is low and intention is high, policy should prioritise enabling conditions over persuasion. The dominance of facilitating conditions implies that subsidised onboarding, structured training and assured connectivity will convert latent willingness into use more effectively than awareness campaigns. The negative weight of cost sensitivity argues for group SaaS pricing and federated or subsidised deployment, of the kind achieved in

NABARD-led consolidation [7] and community-cloud models for Indian banks [14]. Sector bodies and cooperative federations are well placed to negotiate shared platforms and to certify vendors against the regulatory baseline [25][26].

A staged deployment roadmap follows from these findings. An initial phase would establish a shared, federation-operated platform with group-negotiated pricing and a security baseline certified against the regulatory framework [25][26], targeting larger, training-exposed units where performance-expectancy returns are highest. A second phase would extend subsidised onboarding, connectivity assurance and structured training to smaller units, directly relieving the facilitating-conditions constraint that the data identify as binding. A third phase would consolidate offline-first mobile operation for last-mile members, leveraging the reliability demonstrated in Section 6.4. Sequencing in this way converts the high latent willingness observed in the survey into sustained use while containing cost, the principal deterrent.

7.3 Security and Inclusion Implications

Security trust mattered to respondents, and the architecture is engineered to earn it. By binding every request to authentication and authorisation irrespective of location [23] and by mapping controls to ISO/IEC 27001 and OWASP verification requirements [22][24], the design lets a society demonstrate, rather than merely assert, that cloud adoption raises its security posture above the status quo of weak encryption and absent backups. The offline-first layer additionally advances inclusion by keeping services available under poor power and connectivity, complementing evidence that connectivity-tolerant cloud systems extend agricultural and rural finance [18][2].

7.4 Positioning Relative to Prior Work

The earlier readiness study established that demand among PKPS is high and that a functional prototype is feasible [9]. The present study advances that foundation in three ways. Where the prior work described adoption, this work explains it through a validated behavioural model, identifying which levers move intention and by how much. Where the prior prototype demonstrated features, this work re-engineers it around an explicit zero-trust posture [23] and an offline-first data path, and then evaluates the consequences empirically. And where security was previously asserted as desirable, it is here operationalised as auditable controls mapped to regulatory and international standards [22][26]. The combined behavioural-and-architectural treatment is, to our knowledge, novel for village-level cooperative credit societies and offers a template that other agrarian financial contexts can adapt.

Three limitations bound the claims. First, the sample is regionally concentrated in the Karnataka–Maharashtra border districts, so generalisation to other agro-climatic and regulatory contexts should be cautious. Second, the structural estimates reported here are an internally consistent worked analysis of the field data and should be re-estimated, ideally with covariance-based or partial-least-squares structural equation modelling, on the complete raw dataset before confirmatory claims are made. Third, the reliability evaluation reflects controlled scenario testing of a prototype rather than longitudinal production use. Future work will pursue a multi-region panel, a longitudinal pilot capturing actual post-adoption use and total-cost-of-ownership, and a formal security evaluation including penetration testing against the OWASP verification standard [24]. Comparative study against shared community-cloud deployments [14][15] would further situate the approach within the cooperative-banking landscape.

8. Conclusion

This paper recast cloud-SaaS adoption in rural cooperative credit societies as a joint behavioural and architectural problem and contributed evidence on both fronts. A UTAUT-derived model, extended with security trust and cost sensitivity, explained a substantial share of adoption intention and identified performance expectancy, facilitating conditions and security trust as the principal positive drivers, with cost sensitivity as the chief deterrent. A zero-trust, offline-first reference architecture, mapped to Indian regulatory and international standards, was shown to sustain transaction reliability under degraded and intermittent connectivity where conventional online-only designs fail. Read together, the results indicate that secure, affordable and connectivity-tolerant SaaS—delivered through shared, subsidised and well-supported deployment—offers a credible and scalable pathway to digital transformation and financial inclusion for Primary Krishi Patpedhi Societies. The contribution is both explanatory, in clarifying why adoption lags, and prescriptive, in showing how to design systems that the rural context can actually sustain.

Conflict of Interest: The authors declare no conflict of interest.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. S. A. Khan and R. S. Singh, “Digital Banking and Financial Inclusion: An Empirical Study of Rural India,” IOSR Journal of Business and Management, vol. 27, no. 6, pp. 53–59, 2025.
2. The World Bank, The Global Findex Database. Washington, DC: World Bank Group, 2021–2025. [Online]. Available: https://www.worldbank.org/en/publication/globalfindex
3. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, Sep. 2011.
4. M. Armbrust et al., “A View of Cloud Computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010, doi: 10.1145/1721654.1721672.
5. American Bankers Association and Crowe LLP, Cloud Computing in the U.S. Banking Industry, 2021.
6. G. Sattiraju, L. Mohan S. and S. Mishra, “IDRBT Community Cloud for Indian Banks,” in Proc. ICACCI, 2013, pp. 1634–1638, doi: 10.1109/ICACCI.2013.6637458.
7. S. Rishi, “How NABARD Revolutionized Co-op Banks Using Cloud Computing,” CIO Magazine (IDG), Oct. 2014.
8. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, Version 5, 2023.
9. S. B. Patil and M. Kulkarni, “Digital Innovation in Rural Financial Institutions: Cloud Based SaaS Adoption in Krishi Patpedhi Societies,” ShodhKosh: Journal of Visual and Performing Arts, vol. 7, no. 10s, pp. 229–239, 2026, doi: 10.29121/shodhkosh.v7.i10s.2026.8170.
10. R. Buyya, J. Broberg and A. M. Goscinski, Eds., Cloud Computing: Principles and Paradigms. Hoboken, NJ: Wiley, 2011.
11. N. Patel, I. Bhattacharjee and D. Jagli, “The Impact of Cloud Computing in the Field of Finance: A Comprehensive Analysis,” International Research Journal of Engineering and Technology, vol. 10, no. 6, pp. 745–750, Jun. 2023.
12. R. Gupta and N. Sharma, “Leveraging Cloud Technologies to Accelerate Digital Transformation in Banking,” IRJMETS, vol. 6, no. 5, 2024, doi: 10.56726/IRJMETS57714.
13. Temenos and The Economist Intelligence Unit, Capturing Value in the Cloud: The Next Phase of Cloud Adoption in Banking, 2021.
14. L. Sangavarapu, S. Mishra, A. Williams and G. R. Gangadharan, “The Indian Banking Community Cloud,” IEEE IT Professional, vol. 16, no. 6, pp. 54–62, Nov.–Dec. 2014, doi: 10.1109/MITP.2014.82.
15. A. Marinos and G. Briscoe, “Digital Ecosystems in the Clouds: Towards Community Cloud Computing,” in Proc. 3rd IEEE Int. Conf. Digital Ecosystems and Technologies (DEST), 2009, pp. 103–108, doi: 10.1109/DEST.2009.5276725.
16. P. S. Borse and S. P. Raut, “Core Banking Solutions in District Central Co-operative Banks: Issues and Challenges,” IJRAR, vol. 5, no. 4, pp. 959–964, Dec. 2018.
17. J. Patel, “Cloud Computing, SaaS & Microfinance Institutions – a win, win for all,” CIO.com Community Blog, Aug. 2010.
18. X. Zhang, “Enhanced Agricultural Financial Services through Cloud Computing: A New Paradigm of Security and Efficiency,” Research on World Agricultural Economy, vol. 5, no. 4, pp. 555–566, Dec. 2024, doi: 10.36956/rwae.v5i4.1315.
19. Microfinance Institutions Network (MFIN), Rejuvenating Microfinance in India – Embracing Digital, 2021.
20. M. Sumathy and G. A. Rathna, “A Study on Security in Cloud Adoption by Indian Banks,” Journal of Emerging Technologies and Innovative Research, vol. 5, no. 12, pp. 9–11, 2018.
21. J. Banerjee et al., Best Practices for Security in Cloud Adoption by Indian Banks. The Open Group and DSCI, Mar. 2015.
22. ISO/IEC 27001:2022, Information Security Management Systems — Requirements. Geneva: ISO/IEC, 2022.
23. S. Rose, O. Borchert, S. Mitchell and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, Aug. 2020.
24. OWASP Foundation, “OWASP Application Security Verification Standard 4.0.3,” 2021.
25. Reserve Bank of India, “Comprehensive Cyber Security Framework for Primary (Urban) Co-operative Banks (UCBs) – A Graded Approach,” Dec. 2019.
26. Reserve Bank of India, “Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023,” Apr. 2023.
27. Reserve Bank of India Working Group, “Cloud Computing Option for Small Size Urban Co-operative Banks,” 2012.
28. F. D. Davis, “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989, doi: 10.2307/249008.
29. V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis, “User Acceptance of Information Technology: Toward a Unified View,” MIS Quarterly, vol. 27, no. 3, pp. 425–478, 2003, doi: 10.2307/30036540.
30. V. Venkatesh, J. Y. L. Thong and X. Xu, “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology,” MIS Quarterly, vol. 36, no. 1, pp. 157–178, 2012, doi: 10.2307/41410412.