DIGITAL PORTFOLIOS OF THE POOR

Philosophies of Trust within Digital Financial Lives

Nigeria • Kenya • India • Pakistan

2024–2026

Prepared by Decodis in partnership with the Henry J. Leir Institute at Tufts University

Executive Summary

Daily mobile phone use has grown substantially across the Global South along with social media, videos, voice and text messages. But use of digital financial tools has lagged. Digital financial service providers often lament that customers lack trust, but digital trust has remained poorly defined and therefore unclear how to enhance. This study set out to change that.

Across Nigeria, Kenya, India, and Pakistan, the Digital Portfolios of the Poor project surveyed over 3,400 men and women on their digital trust philosophies. Responses were largely open-ended voice responses, capturing qualitative perspectives often drowned out in traditional quantitative surveys. Data were collected through asynchronous IVR voice, with open-ended responses analyzed using AI-powered thematic coding. This is a qualitative research-at-scale approach rarely deployed in digital inclusion research.

Over the course of analyzing these data, it became clear that a portfolio is not just a record of transactions. It is also a map of relationships, obligations, and trust. To understand the digital portfolios of the poor is to understand who they trust, and why.

Across all four countries, the same three archetypes of digital trust philosophy emerged: Assurance Seekers, Protection Seekers and Control Seekers — grounded in four common pillars of trust: Risk Perception, Risk Mitigation, Responsibility Perception and Benefit Perception.

The archetypes are globally consistent, but their proportions and characteristics differ meaningfully by country, reflecting different digital maturity levels, product ecosystems, and cultural contexts. A key cross-country finding: while the archetypes are universal, the primary benefit of digital tools and the primary source of perceived risk differ significantly across countries. For example, in Kenya and Nigeria, market reach and income generation are key motivators. In India and Pakistan, convenience dominates. Risk also differs: in Nigeria and Kenya, scams dominate; in Pakistan, the primary risk is a lack of digital literacy itself.

Most critically, however, we wanted to see if using these archetypes allowed digital financial service providers to develop strategies to build digital trust across the full range of their clients, from the most anxious to the most confident. By running tightly focused workshops, we leveraged the deep personas and audios that came out of the research to ignite ideas across organizations that gave institutions opportunities to enhance trust for their customers.

I. Why did we feel we needed a new way to understand digital trust?

This study addresses the gap between digital access and digital financial use across the Global South. While mobile phone use has grown substantially, digital financial tool adoption has consistently lagged — and the trust barriers behind this gap have remained poorly understood and poorly measured.

We bring a new analytical lens to this challenge. Traditional segmentation measures who is digitally active, and why. Most digital inclusion research uses inductive segmentation: grouping users by who uses what, how often, or on which channels. Resulting strategies involved crafting interventions to move users "forward" on some digital journey. This approach is useful for mapping activity, but it reveals little about the why and how behind digital behaviors.

Digital engagement is not only about access or skills. It is fundamentally about trust – how users perceive risk, build confidence, and decide to engage or withdraw. Traditional segmentation based on usage misses the invisible architecture of trust. For example, two people might both use mobile money, but one does so only after triple-checking with their bank and friends, while the other simply accepts things as they are. Standard segments would group these two together, missing the radically different trust philosophies and, therefore, the different types of support they need.

Qualitative-style inductive analysis unearths not usage profiles, but trust philosophies shaping every digital action, risk, and expectation. Traditional segmentation makes the digital landscape look flat. Trust philosophy segmentation reveals its contours. Each group looks similar on the surface, but their risk perceptions, barriers, motivators, and intervention needs are fundamentally different.

Research Objectives

- Develop a globally relevant framework of digital trust philosophies as described from the perspective of actual and potential users.
- Determine if there are commonalities across countries, segments, phone ownership or other digital service use.
- Test whether these frameworks help digital service providers generate ideas about how to increase trust.

II. Methodology: Qualitative Data at Scale

Why Qualitative Data?

Trust is a nebulous, qualitative idea which needs to be described in an open-ended response. Quantitative questions ask respondents pre-conceived answers — this study was designed to be open to new perspectives. The approach asked open-ended questions such as:

- Whose responsibility is it to make sure that users don't experience privacy breaches or security risks?
- How do you think security and privacy breaches happen?
- What do you see as pros and cons of using digital financial services?

A large sample was needed to determine whether trust deficits differ systematically across segments and to ensure findings were not spurious but would apply to a broad range of customers of digital financial service providers.

Data Collection Across Four Countries

Data was collected using asynchronous IVR (Interactive Voice Response) surveys and web links in each country. Pre-recorded, local language-speaking voice actors — not AI-generated voices — conducted interviews. This removed interviewer interruption and social desirability bias, producing responses that were typically three times longer than typical in-person interview responses.

Country	Languages	Sample	Modules/Questions
Kenya	Swahili, Luo, Kalenjin, Turkana	992 respondents	7 modules, 280 voice + 166 keypad questions
Nigeria	Hausa, Yoruba, Igbo	960 respondents	4 modules, 133 voice + 94 keypad questions
India	Hindi, Tamil, Telugu	939 respondents	8 modules + 191 voice + 113 keypad questions
Pakistan	Urdu, Punjabi	544 respondents	4 modules + 356 questions

The survey instrument

The survey is organized into seven modules, administered one per week over seven weeks via automated voice call. Each module combines keypad responses to capture quantitative prevalence with open-ended voice responses to capture qualitative nuance. Respondents do not need to be literate to participate — all questions are pre-recorded by local voice actors in the respondent's own language. The modules are as follows:

- **Survey 1 — Demographics and device access:** The opening module establishes the foundation of each respondent's digital portfolio. It collects demographic information including location, age, gender, education, and income, before moving to a detailed exploration of every digital device the respondent has access to — including devices they borrow or share. For each device, the module asks about ownership, SIM card registration, internet connectivity, camera and audio use, and privacy concerns. This module also introduces the survey structure and consent process.
- **Survey 2 — Social media and messaging platforms:** This module explores respondents' use of WhatsApp, YouTube, Facebook, Instagram, and Twitter — covering how often they use each platform, what for, whether they use their own accounts, and what privacy or identity concerns they hold. It also asks about photo editing and file-sharing apps, exploring whether respondents have files or images they are concerned about others accessing.
- **Survey 3 — Digital financial services:** This module covers the full range of digital financial activity — mobile banking, mobile payments, pay-as-you-go services, mobile lending, mobile savings, community savings and lending groups, and cash kept at home. For each, the module asks how respondents use the service, what they worry about, and who they are concerned might access their financial information.
- **Survey 4 — Other digital services:** This module explores a broader range of digital activity including email, entertainment platforms, news consumption, online gaming, online shopping, online betting, government service platforms, and ride-hailing apps. For each, respondents are asked about frequency of use, devices and connectivity, privacy concerns, and any worries about others knowing what they are doing online.

Using Skits to Increase Qualitative Depth

Each country used 4–6 fictional audio skits, each followed by 8 questions. Respondents listened to scenarios and shared their thoughts. Skits allowed people to discuss sensitive or abstract topics like trust in a depersonalised way, making nebulous concepts concrete. Examples included scam scenarios, mobile money disputes, and in Pakistan, a BISP beneficiary being charged unauthorised fees by a payment agent.

Each survey incorporates six skits in Kenya and four to six skits in India, Nigeria and Pakistan, each followed by eight questions. Audio skits are short, pre-recorded audio stories featuring fictional characters navigating everyday situations. Rather than asking a respondent directly about their own experiences, the study plays a story about someone else in a similar situation and asks what they think. Because respondents are reacting to a character rather than speaking about themselves, they are more likely to share honest perspectives, and nebulous concepts are made concrete.

In Kenya, for example, one skit depicts a market character named Peter going to buy items from Moraa, who refuses mobile money due to an outstanding mobile loan and insists on cash. In India, a skit shows a character named Rajeev receiving an SMS claiming he has won a lottery prize, with his uncle warning him it is a scam. Respondents are only ever exposed to audio versions of the skits via phone call; video versions exist solely for illustration and translation purposes.

- **Survey 5 — Audio skits: mobile scams and digital loans:** The first skit-based module introduces two fictional audio stories. The first depicts a woman receiving a suspicious call from someone claiming to be from a mobile network, with a friend suggesting it could be a scam. Respondents are asked about their own experiences with similar situations, who they believe are responsible for protecting people from scammers, and whether they would pay for a scam protection service. The second story follows a woman who needs money and is considering a digital loan she is unsure she can repay on time. Respondents are asked about the benefits and risks of digital lending, the role of credit reference bureaus, and which they consider worse — falling victim to a mobile scam or being blacklisted for loan default.
- **Survey 6 — Audio skits: fake news and automatic loan deductions:** The second skit-based module presents two further stories. The first follows two people debating whether a news story circulating on social media is true. Respondents are asked how they judge the truthfulness of online news, whose responsibility it is to verify it, and whether the benefits of getting news online outweigh the risks of misinformation. The second story follows a woman who has taken a digital loan and is considering stopping mobile money payments to avoid automatic deductions, putting her business at risk. Respondents are asked about lenders' power to make automatic deductions, the advantages and disadvantages of digital versus personal lenders, and what they would do in the same situation.
- **Survey 7 — Audio skits: online harassment and data privacy:** The final module presents two closing stories. The first follows a woman considering selling products online after hearing about the harassment another woman has experienced from customers on digital platforms. Respondents are asked about their own or others' experiences of online harassment, who is responsible for women's safety in online business, and how worried they are about delivery and payment disputes in online commerce. The second story follows two people discussing how a video platform seems to be recommending content based on their recent activity. Respondents are asked about their understanding of how algorithmic recommendations work, how they feel about platforms using their behavior to generate revenue, and which they consider worse — being subject to data exploitation or experiencing online harassment. This

module concludes the survey, and respondents receive their compensation on completion.

III. The Four Pillars of Digital Trust

Through inductive analysis grounded in participants' own words, four key pillars of digital trust were identified.

These pillars did not emerge from pre-defined categories but were derived inductively from respondents' own language across all four countries. Open-ended voice responses were coded thematically, and cross-sectional pattern analysis revealed four consistent dimensions through which people experience, evaluate, and act on digital trust. The sections below explain the analytical approach used to surface these pillars and the rationale for each one.

A Trust-Centered Analytical Framework

The study captured how users perceived, managed, and acted upon trust and risk across four critical areas:

- **Risk perception:** What are people truly worried about? (e.g., hacking, scams, failure, theft)
- **Risk mitigation:** What do people *actually do* to protect themselves? (e.g., external confirmation, cautious sharing, monitoring)
- **Responsibility perception:** Who do they believe should keep them safe – institutions, platforms, themselves, or others?
- **Benefit perception:** What makes digital services worth the risk? (e.g., time saved, income, ease, safety)

By collecting data across these four windows into their lived realities, we ran a cluster analysis that looks beyond what people do and reveals *how* and *why* different people *trust*.

This approach uncovered *natural groupings* – segments are not forced but emerge based on patterns in how people weigh risk, take precautions, assign responsibility, and see value.

Each cluster is a distinct trust profile: Not just a behavioral group, but a reflection of a deeper, guiding trust philosophy:-

- Some users only trust after actively checking and verifying.
- Others simply accept digital risk as a fact of life.
- Another group pursues inclusion on their own terms, by taking personal control.

By identifying these unique trust and risk management philosophies, practitioners and designers can build interventions, protections, and communications that resonate – speaking the language of trust that users actually use.

Analytical Framework: Four Steps from Data to Archetypes

To create digital trust philosophies out of an enormous set of open-ended text and audio data, we followed four steps:

1. **Multi-dimensional Data Integration:** We systematically synthesized respondents' open-ended responses to questions across four core dimensions: *Risk Perception, Risk Mitigation Behaviors, Responsibility Perception and Benefit Recognition. This ensures a holistic capture of trust-related attitudes and behaviors.*

2. **Thematic Analysis - Systematic Inductive Coding:** Using iterative, grounded coding techniques, we inductively identify thematic categories and subcategories across all four pillars. This qualitative approach unravels not only surface concerns, but also latent, recurrent themes embedded in diverse user experiences.

3. **Latent Profile Derivation through Qualitative Comparative Patterning:** We conduct cross-sectional pattern analysis across coded data to qualitatively derive emergent trust profiles, identifying meaningful clusters of respondents based on distinct patterns of trust formation, risk response, and benefit expectation.

4. **Empirical Validation via Agglomerative Cluster Analysis:** To validate and solidify the qualitative typology, we employ agglomerative hierarchical clustering to empirically test the robustness and reproducibility of the emergent clusters along the full suite of coded variables.

The Rationale for the Four Pillars

Risk Perception: Trust begins with awareness. People's readiness to use digital tools depends on what dangers they foresee, whether that's hacking, scams, or technical failures. Mapping risk perception allows us to capture why some users hesitate while others proceed – revealing the emotional and cognitive triggers that open or close the door to digital adoption.

Risk Mitigation: Trust is more than belief; it is enacted through daily choices. By examining risk mitigation strategies – like cautious sharing and external verification – we get granular insight into how users translate their fears or confidence into practice. This dimension reveals not just theoretical trust, but trust-in-action.

Responsibility Perception: Trust is deeply social and institutional. Whether users trust a system often hinges on who they believe is accountable for security – banks, government, platforms, or themselves. By including responsibility perception, we surface the implicit contracts and expectations that frame people's willingness to engage.

Benefit Perception: Trust is not only about reducing risk, but about pursuing value. Users weigh risks against perceived benefits: income opportunities, convenience, safety, or cost savings. This dimension grounds trust in lived realities and practical utility – capturing why digital services are worth the leap of faith.

Note on Risk Mitigation in Kenya

Risk Mitigation was excluded from the clustering process in Kenya. Unlike in the other three countries, users across all Kenyan archetypes described near-identical mitigation behaviours, most often reciting M-PESA fraud prevention guidance almost word for word. This pattern did not meaningfully differentiate the clusters. This may be a reflection of Kenya's long history of mobile money use and the strong public safety messaging by Safaricom.

IV. Digital Trust Archetypes: A Global Framework

Cluster analysis of the four pillars revealed three distinct archetypes of digital trust philosophy across all four countries. Along this spectrum, each step represents a meaningful shift in how much agency users feel they have over their own digital safety and therefore a fundamentally different starting point for any trust-building intervention.

AS Assurance Seekers	PS Protection Seekers	CS Control Seekers
Less trust & confidence	Some trust & confidence	More trust & confidence

AS ASSURANCE SEEKERS	They have limited understanding of risks and mitigation, building trust through peer assurance. Less trust and confidence. They engage with digital tools by habit or social familiarity rather than informed choice.
PS PROTECTION SEEKERS	They have the widest range of fears, increasing the likelihood of withdrawing from digital tools. They build trust through provider or government protection. Some trust and confidence.
CS CONTROL SEEKERS	Digitally competent and confident in their ability to self-protect. More trust and confidence. They take primary responsibility for their own protection and actively implement digital safety strategies.

V. Kenya

Sample and Context

Kenya is the most digitally mature country in the study, with near-universal mobile money adoption driven by M-PESA. The Kenyan sample drew on 992 respondents across six regions: Kisumu, Kericho, Nairobi, Mombasa, Malindi, and Turkana County. Interviews were conducted in Swahili, Luo, Kalenjin, and Turkana.

992	6	58%	60%
Respondents	Regions	Women	Control Seekers

Archetype Distribution

CS
60%
CONTROL SEEKERS

The most digitally confident group. High smartphone users. Concerned primarily about scams and auto-deductions from their mobile wallet. They place responsibility for their digital financial protection on themselves but on the government for online safety. Digitally assertive, highly intentional, wanting visibility and recourse when something goes wrong. Many use WhatsApp for business and digital loans. Primary benefit: market reach (50%) and financial access (40%).

AS
39%
ASSURANCE SEEKERS

The least aware and least confident users. Highest share of feature phone access in the sample. Focused primarily on mobile money for basic remittance needs. Digital benefit centered on financial inclusion — being part of the financial world. Little understanding of what digital risks exist and largely unsure of who is responsible for protecting them. Primary benefit: financial access (60%).

PS
1%
PROTECTION SEEKERS

A very small but distinct group. Most concerned about scams. Look for Safaricom to keep them safe. Primary benefit: market reach (66%).

Kenya-Specific Findings

Risk Mitigation as a Shared Script

Unlike in other countries, risk mitigation did not differentiate trust archetypes in Kenya. Across all groups, respondents described the same behaviours — verifying numbers, reporting fraud, blocking suspicious contacts — and many recited M-PESA fraud prevention instructions almost verbatim. This reflects the depth of Safaricom's public safety messaging.

A Uniquely Kenyan Risk: Theft by Family and Friends

Kenyan respondents raised a concern that did not appear in any other country: the fear that family members or friends with access to a shared phone could steal from their M-PESA account without their knowledge. This is a product of the high phone-sharing rates in the sample.

Online Banking Gender Gap

Online and mobile banking use was notably higher among men (52%) than women (39%), despite near-universal M-PESA adoption across genders. This gap may reflect greater concern among women that money saved digitally could be stolen.

Key Kenya summary: Financial scams are the dominant risk concern across all archetypes. The majority of Assurance Seekers are unclear about who is responsible for their digital safety. Financial access is the primary perceived benefit of digital tools. Kenya has the highest proportion of Control Seekers of all four countries in the study, reflecting its long history of digital financial use.

VI. Nigeria

Sample and Context

Nigeria has seen strong growth in digitally-enabled account ownership and is characterised by a vibrant informal digital economy driven by WhatsApp-based commerce. The Nigerian sample drew on 960 respondents. Three digital financial service providers participated in co-design workshops following the research.

960	47%	36%	17%
Respondents	Assurance Seekers	Control Seekers	Protection Seekers

Archetype Distribution

AS 47% ASSURANCE SEEKERS

Limited awareness of digital risks. Engage with digital tools by habit or social familiarity. Rely on peer verification rather than institutional guidance when something goes wrong. Build trust through the reassurance of people around them rather than their own knowledge.

CS 36% CONTROL SEEKERS

The most digitally confident group. Take primary responsibility for their own protection and actively implement digital safety strategies. The only Nigerian archetype to mention transaction monitoring. Demand visibility and recourse from telecoms and platforms.

PS 17% PROTECTION SEEKERS

Aware that digital risks exist and have the widest range of fears. Look to institutions and platforms to bear primary responsibility for their safety. More likely to withdraw from digital tools when risks feel unmanaged.

Nigeria-Specific Findings

Institutional Distrust: Middlemen

A uniquely Nigerian concern across all archetypes was fear of middlemen — specifically, bank employees suspected of accessing and misusing customer account details. This form of institutional distrust was not found in any other country in the study.

Transaction Failures

Failures on unstable telecom networks were a meaningful source of anxiety, particularly in payment contexts where a failed transfer damages a user's reputation with the recipient — a social and commercial cost unique to Nigeria's peer-to-peer digital economy.

Market Reach as a Primary Benefit

Unlike India and Pakistan where convenience dominates, Nigerian respondents cited income generation and market reach as secondary drivers alongside convenience — reflecting the importance of WhatsApp-based commerce and the strong link between digital tools and livelihood in the Nigerian context.

Key Nigeria summary: Account hacking and scams are the dominant fear across all archetypes. Transaction failures on unstable networks create a distinctive form of digital anxiety. Convenience is the primary benefit, with income generation a secondary driver — unique to Nigeria's market-oriented digital economy.

VII. India

Sample and Context

India has built remarkable digital infrastructure — hundreds of millions of smartphones and the UPI payments system deployed at scale. But when researchers spoke with 939 Indians across Bihar, Tamil Nadu, Andhra Pradesh, Madhya Pradesh, and beyond, the picture was more uncomfortable. The infrastructure exists, but trust does not.

India had the highest proportion of Assurance Seekers of all four countries, and the government was uniquely identified as the key responsible party for digital protection — a finding not replicated elsewhere.

939	50%	38%	12%
Respondents	Assurance Seekers	Protection Seekers	Control Seekers

Archetype Distribution

AS
50%
ASSURANCE SEEKERS

Half of the Indian sample. These users are not absent from digital life — they use WhatsApp, receive payments, and interact with the digital economy daily. But they do so without understanding the risks they face, without knowing who is responsible for protecting them, and without the tools to act when something goes wrong. 68% could not say who should be responsible for their digital safety. More than half could not describe a single action they would take if something went wrong. They navigate digital life by pressing familiar buttons, relying on others to interpret what they don’t understand.

PS
38%
PROTECTION SEEKERS

Aware that digital life carries risk. Have absorbed enough of the safety conversation to know they are exposed — but their response is not to act, it is to look upward. 51% believe the government should bear primary responsibility for their online safety. They want protection that arrives without friction, arranged by someone else on their behalf.

CS
12%

Just 12% of the Indian sample. Digitally assertive users who verify before they transact, delete suspicious messages, and hold themselves

CONTROL SEEKERS	accountable for their own safety. Designing for them alone means designing for one in eight.

India-Specific Findings

Borrowed Language, Not Owned Knowledge

A defining characteristic of India's Assurance Seekers was a recurring pattern: they had absorbed fragments of messaging — a half-remembered warning, a notice on a bank wall — but could not make it their own. When asked about risk, they reached for borrowed language. When asked who should protect them, they went quiet.

Government as the Key Responsible Party

More than in any other country, Indian respondents — particularly Protection Seekers — identified the government as the primary responsible party for digital safety. 51% of Protection Seekers cited government responsibility. This reflects India's context of cybercrime helplines like 1930 and evolving regulatory frameworks.

Convenience as a Universal Draw

Across all three groups, convenience was the universal draw — more so than in comparable countries like Kenya, where market opportunity ranks higher. This means that building trust in India starts not with expanding capabilities, but with making existing digital experiences feel safer and simpler.

Key India summary: India has the highest proportion of Assurance Seekers of all four countries. The government is uniquely identified as the key responsible party. Convenience dominates as the primary benefit. Infrastructure and access are not the barriers — trust is.

VIII. Pakistan

Sample and Context

Pakistan presents the most acute digital financial inclusion challenge in the study. Uptake in digitally-enabled accounts, payments, and storage are all weak across the board. The Pakistani sample drew on 544 respondents across six cities in Punjab province, interviewed in Urdu and Punjabi.

544	40%	38%	22%
Respondents	Assurance Seekers	Protection Seekers	Control Seekers

Archetype Distribution

AS
40%
ASSURANCE SEEKERS

Respondents have a hard time articulating what they believe risks are and what mitigation is possible. They cannot imagine what is happening digitally beyond the routine patterns of keystrokes. Entirely unable to articulate who is responsible for protecting them (100%). Their primary mitigation strategy is to learn slowly (56%). Their biggest perceived benefit is easy communication (47%).

PS
38%
PROTECTION SEEKERS

Recognise risks but rely on agents and personal responsibility to protect them. Verification is the dominant mitigation behaviour (48%). Personal responsibility (40%) and agents (33%) are the most cited sources of protection. Biggest benefit is convenience (67%).

CS
22%
CONTROL SEEKERS

Aware of digital risks but a significant proportion (33%) deny that any risk exists. Verification is the dominant mitigation behaviour (61%). 97% hold themselves personally responsible. Biggest benefit is convenience (83%) — the strongest convenience signal of any archetype across all four countries.

Pakistan-Specific Findings

Agents as the Key Responsible Party

Unlike India where government is the key responsible party, in Pakistan agents play that role — particularly for Protection Seekers. Agents are seen as intermediaries who help navigate and explain digital tools. This reflects Pakistan's agent-heavy financial services ecosystem, including BISP payment agents.

Digital Literacy as the Primary Risk

In Kenya and Nigeria, scams dominate as the primary risk perception. In Pakistan, the primary concern is users' own lack of digital literacy — a fundamentally different and more structural barrier that points to a different set of interventions.

Easy Communication for Assurance Seekers

While convenience dominates as the primary benefit across Protection and Control Seekers, Pakistan's Assurance Seekers are primarily drawn by easy communication — a finding more similar to the community-connection orientation seen in some other countries than to the market-reach orientation of Kenya and Nigeria.

Key Pakistan summary: Digital literacy — not scams — is the primary perceived risk. Agents are uniquely important as both intermediaries and protectors. Pakistan has the most evenly distributed archetype split of all four countries, with no single archetype dominating.

IX. Cross-Country Conclusions

What the Four Countries Tell Us

Inductive analysis of digital trust across four countries manifested four common pillars, which statistically clustered into three archetypes. The archetypes are universal — but their proportions, characteristics, and the specific fears and motivations underpinning them differ meaningfully by country.

	Kenya	Nigeria	India	Pakistan
Assurance Seekers (AS)	39%	47%	50%	40%
Protection Seekers (PS)	1%	17%	38%	38%
Control Seekers (CS)	60%	36%	12%	22%
Sample size	992	960	939	544
Primary benefit	Market reach	Convenience / income	Convenience	Convenience / communication
Primary risk	Scams	Scams / account hacking	Scams	Digital literacy
Key responsibility	Telecoms (Safaricom)	Institutions / self	Government	Agents / self

Archetype Comparisons Across Countries

Assurance Seekers

Present in all four countries, ranging from 39% in Kenya to 50% in India. Consistently the least digitally confident group, relying on community guidance and peer assurance. However, the nature of their engagement differs: in Kenya and Nigeria, they engage by habit. In India, they have absorbed fragments of safety messaging but cannot make it their own. In Pakistan, they cannot even imagine what is happening digitally beyond routine keystrokes.

Protection Seekers

Represent a very small share in Kenya (1%) but 38% in both India and Pakistan. Who they look to for protection differs sharply by country: the government in India, agents in Pakistan, and institutions/platforms in Nigeria. This reflects each country's specific institutional landscape.

Control Seekers

Most prevalent in Kenya (60%), reflecting its long history of digital financial use. Least prevalent in India (12%). In all countries, they hold themselves primarily responsible for their own protection and use verification as their primary mitigation strategy. In Kenya, they look to Safaricom. In Pakistan, they are the most strongly self-reliant, with 97% attributing responsibility to themselves alone.

Cross-Country Benefit and Risk Patterns

- Benefits: Market reach and income generation dominate in Kenya and Nigeria. Convenience dominates in India and Pakistan. Easy communication is uniquely prominent for Pakistan's Assurance Seekers.
- Risks: Scams dominate in Kenya and Nigeria. Scams are also primary in India alongside digital literacy concerns. In Pakistan, digital literacy is the primary concern across all archetypes — a more structural barrier than in other countries.
- Responsibility: Telecoms (Safaricom) in Kenya. Institutions and self in Nigeria. Government in India. Agents and self in Pakistan.

Why This Approach Is Different

As described in Section I, this study's trust-philosophy approach differs fundamentally from traditional inductive segmentation, which groups users by behavior and channel but reveals little about the underlying reasons people engage or withdraw from digital tools. The cross-country findings above demonstrate that this distinction is not merely theoretical: identical usage behaviors can mask radically different trust philosophies — and therefore entirely different intervention needs.

Digital engagement is not only about access or skills. It is fundamentally about trust — how users perceive risk, build confidence, and decide to engage or withdraw. Trust philosophy segmentation reveals the contours of the digital landscape that usage data alone cannot see.

X. Application: Provider Workshops in Kenya and Nigeria

To translate the Digital Trust Philosophy archetypes from research insight into institutional action, Decodis conducted a series of applied workshops with digital financial service (DFS) providers in Kenya and Nigeria. The objective was practical: to help institutions develop tractable, implementable solutions that build trust across all three archetypes – not just for the most digitally confident segment of their customer base.

Two foundational principles guided the workshop design. First, solutions developed for multiple archetypes are more effective at growing customer trust overall than those designed for a single profile. Serving only one archetype risks deepening the trust gap for others. Second, because providers operate across multiple teams with competing priorities, the workshops were designed to surface solutions that could enter project pipelines across the organization – earning trust by layering interventions across functions rather than relying on a single initiative.

Participating Institutions

Workshops were conducted with six institutions across the two countries, selected to represent a range of provider types and levels of digital maturity.

In Kenya, **three SACCOs – Stima SACCO, a second cooperative, and Mwalimu National –** participated. These are bottom-of-the-pyramid savings and loan institutions in the early stages of digitizing their services, making them an ideal context for exploring how trust-building can be embedded into the digitization process from the outset.

In Nigeria, **three providers participated: Ajocard,** a payments product; **Source Microfinance Bank,** a digital-first bank; and **Esusu Africa,** a savings group fintech. Together, they represent distinct segments of the Nigerian DFS landscape, from informal savings to formal digital banking.

Examples: Multiple Solutions Across Many Teams

Each workshop generated a range of concrete solutions, organized by organizational function. The examples below illustrate the depth and breadth of ideas that emerged when provider teams engaged directly with the archetype framework.

Kenya – Stima SACCO. The Legal and Compliance team identified an in-app dispute clarity button linked to the CRM system, enabling members to track and resolve loan issues seamlessly. The Branch and Finance team proposed flexible daily and weekly repayment options alongside an Apple Store-style genius bar for hands-on member support. The Customer Experience team generated three complementary ideas: a community Q&A support button for peer-guided reassurance; app-based loyalty and referral incentives to reward engagement; and offline access features combined with local reassurance mechanisms specifically designed for the institution's most vulnerable members.

Nigeria – Ajocard. Across six organizational areas, Ajocard's teams developed a suite of trust-building measures. Compliance proposed safety-check prompts after each savings transaction, treating user feeling as a measurable metric. Leadership committed to tracking and reporting a User Trust Index as a board-level priority. Customer Experience recommended weekly feedback pulse checks to ensure smooth, uninterrupted user interactions. Business Development identified trusted everyday networks as a distribution and uptake channel. Product Development proposed layered user journeys with guided onboarding for new users and simplified, safe pathways for all. Marketing committed to co-creating campaigns with real users, drawing on their lived trust deficits to make communications authentic and relevant.

These examples illustrate a consistent pattern across all six institutions: when provider teams engage with the archetypes through concrete audio examples and real customer voices, they generate not one or two ideas but a pipeline of solutions spanning functions. The archetypes serve as a shared language that connects customer reality to institutional priorities.

XI. Conclusions

The four-country study, and the provider workshops that followed, point to four overarching conclusions for the field of digital financial inclusion.

There is no monolithic digital trust philosophy, even within countries or segments. Every country studied contains all three archetypes. Even where one archetype predominates – Control Seekers in Kenya, Assurance Seekers in India – the others are present in meaningful proportions. Providers who design for a single profile will always leave a significant share of their customers underserved.

A new methodology generates qualitatively informed insights at quantitatively meaningful scale. The combination of open-ended voice data collection and AI-powered thematic coding made it possible to identify a cross-country set of four trust pillars while still revealing sub-themes specific to each country's supply-side dynamics and socio-economic context. This format of data was critical to findings that are simultaneously universal and locally differentiated.

Archetypes ranged from confused to confident. India and Pakistan have the highest proportions of Assurance Seekers – users who are uncertain, disoriented, or lacking the foundational literacy to navigate digital finance independently. Kenya and Nigeria have higher proportions of confident Control Seekers, but Assurance Seekers are a substantial minority in both. No country has "solved" digital trust, and even the most digitally mature markets carry a significant share of users who remain in need of structured reassurance.

Provider workshops generate multiple tractable solutions, suitable for serving all archetypes of customers. Working with concrete archetype examples, audio clips, and participant materials galvanizes trust-building ideas and enables focused workshops in which senior staff can meaningfully participate. It is critical to engage managers with the internal

authority to move ideas into project pipelines. When this condition is met, a single workshop can generate a roadmap of implementable interventions spanning compliance, product, marketing, and customer experience – each one grounded in the actual trust philosophies of the customers the institution serves.

DECODIS®

Social Research. Reimagined.

www.decodis.com
info@decodis.com
linkedin.com/company/decodis
@decodisresearch