



ORIGINAL RESEARCH ARTICLE

**Governance-Centered Digital Trust in Developing Countries:
Developing and Validating an Indigenous Digital Trust Model for Iran
Using a Mixed-Methods Approach**

Mohammad Reza Pakdel¹, Jalal Haghighat Monfared², Mansoureh Aligholi³

¹ Ph.D. Candidate, Information Technology Management, Islamic Azad University, Central Tehran Branch, Tehran, Iran. Email: mrpakdel1330@gmail.com, 0009-0003-2920-3418.

² Associate Professor, Department of Industrial Management, Islamic Azad University, Central Tehran Branch, Tehran, Iran. (Corresponding Author). Email: J.haghighat@iauctb.ac.ir, 0000-0002-5741-0532.

³ Associate Professor, Department of Business Management, Islamic Azad University, Science and Research Branch, Tehran, Iran. Email: M.aligholi@yahoo.com, 0000-0002-8924-6407.

ARTICLE INFO

Article History:

Received: 2026-06-02

Revised: 2026-07-16

Accepted: 2026-08-28

Published Online: 2026-09-01

Keywords:

Digital Trust; Digital Governance;
Metaverse; Governance-Centered
Trust; Virtual Environments.

Number of Reference: 29

Number of Figures: 0

Number of Tables: 13

DOI:



ABSTRACT

This study aims to develop and validate an indigenous digital trust model tailored to Iran's socio-cultural, legal, and institutional context, with particular attention to emerging challenges of trust in immersive digital environments, including metaverse and virtual platforms. An exploratory sequential mixed-methods design was employed. In the qualitative phase, grounded theory methodology was used with semi-structured interviews of 12 experts (policymakers, senior officials, platform managers, legal specialists, academics) selected via purposive and snowball sampling. Data were analyzed using MAXQDA through open, axial, and selective coding. In the quantitative phase, the model was validated using PLS-SEM via Smart PLS 3 with 100 IT managers (sample size justified by 10-times rule). Qualitative analysis identified 74 concepts, 24 subcategories, and 6 major categories. The core category was governance-centered digital trust. Quantitative results confirmed reliability and validity ($CR > 0.70$, $AVE > 0.50$, $SRMR = 0.058$, $GOF = 0.601$), with all structural relationships significant. The first empirically validated indigenous digital trust framework for Iran, extending theory by conceptualizing trust as governance-centered and identifying institutional fragmentation and accumulated negative experiences as critical determinants. The framework is positioned within the broader context of trust in emerging immersive digital ecosystems. ©authors

► **Citation:** Pakdel, M., Haghighat Monfared, J., Aligholi, M. (2026). Governance-Centered Digital Trust in Developing Countries: Developing and Validating an Indigenous Digital Trust Model for Iran Using a Mixed-Methods Approach. *The International Journal of Metaverse & Virtual Transformation (IJMVT)*, 2(3): 01-20.

Introduction

Digital transformation has fundamentally reshaped the ways governments, businesses, and citizens interact, creating unprecedented opportunities for economic development, public service delivery, and social participation. The rapid diffusion of digital technologies has accelerated the emergence of smart governments, digital economies, electronic commerce, and data-driven policymaking. However, the effectiveness of these developments largely depends on one critical factor: digital trust.

Digital trust refers to stakeholders' confidence in the security, transparency, accountability, fairness, and reliability of digital systems, platforms, and institutions. It functions as a foundational mechanism that reduces uncertainty and encourages individuals and organizations to engage in digital environments. Previous studies have consistently demonstrated that insufficient trust can significantly hinder the adoption of digital services, regardless of the availability of advanced technological infrastructure (Jarvenpaa & Teigland, 2017; Mazhar et al., 2025). Consequently, digital trust has emerged as a strategic prerequisite for achieving sustainable digital transformation.

In recent years, particularly following the COVID-19 pandemic, governments worldwide have increasingly relied on digital technologies to deliver public services, healthcare, education, and administrative processes. This transition has highlighted the importance of digital governance and reinforced the need for trust-based interactions between citizens and digital institutions. Countries with higher levels of digital trust generally demonstrate stronger performance in implementing digital government initiatives, promoting innovation, and expanding citizen participation.

1.1 The Emergence of Immersive Digital Environments and the Metaverse

Beyond traditional digital services, the emergence of immersive digital environments—including the metaverse, virtual reality (VR), augmented reality (AR), and extended reality (XR) platforms—has introduced new dimensions to digital trust research. The metaverse, conceptualized as a persistent, interconnected, and immersive digital universe, represents a paradigm shift in how individuals interact with digital systems and with each other (Dwivedi et al., 2022; Mystakidis, 2022). In these environments, trust extends beyond conventional concerns about data security and privacy to include issues of identity verification, virtual asset ownership, algorithmic fairness, platform governance, and the integrity of immersive experiences (Shin, 2022; Wang et al., 2023).

The metaverse presents unique trust challenges that differ fundamentally from those in traditional digital environments. Users in virtual worlds must trust not only the platform providers but also other users, content creators, and the algorithms that mediate their experiences (Tan & Salo, 2023). Issues such as avatar identity fraud, virtual property theft, manipulative AI-driven interactions, and the concentration of governance power in platform owners raise novel questions about trust formation and institutional accountability (Kitsios & Kamariotou, 2023). Furthermore, the blurring boundaries between physical and virtual realities complicate existing legal and regulatory frameworks, requiring new approaches to governance that can address cross-jurisdictional and cross-dimensional trust relationships (Rauschnabel et al., 2022; Lee et al., 2021).

Given these developments, understanding digital trust in the context of emerging immersive ecosystems has become a critical scholarly and practical concern. The present study, while grounded in the governance realities of Iran's digital landscape, positions its findings within this broader evolution of digital environments, recognizing that the governance-centered trust framework developed here may have relevance for understanding trust dynamics in metaverse and virtual platforms as well.

1.2 International Frameworks and Their Limitations

Several international frameworks have attempted to conceptualize and operationalize digital trust. The World Economic Forum (WEF, 2024) identifies cybersecurity, privacy protection, transparency, accountability, and ethical technology use as the core dimensions of digital trust. Similarly, the European Union's General Data Protection Regulation (GDPR) emphasizes citizens' digital rights, organizational responsibility, and institutional oversight. The National Institute of Standards and Technology (NIST) in the United States focuses primarily on cybersecurity risk management and privacy protection, while the ISACA Digital Trust Ecosystem Framework (2024) adopts a multidimensional perspective that integrates technological, organizational, and human factors.

Despite their valuable contributions, these frameworks have largely been developed within the institutional, legal, and cultural contexts of developed countries. Their direct application in developing countries is often problematic because digital trust is strongly influenced by contextual factors such as governance structures, legal maturity, social capital, cultural values, and citizens' historical experiences with public institutions. Consequently, models designed for highly institutionalized societies may not adequately explain the dynamics of digital trust in countries characterized by regulatory fragmentation, limited institutional trust, and uneven digital development.

1.3 The Iranian Context

Iran represents a particularly important context for investigating digital trust. According to recent international assessments, including the Network Readiness Index (NRI), the E-Government Development Index (EGDI), and the Government AI Readiness Index (GARI), Iran faces substantial challenges in digital governance and public trust. These challenges are associated with several structural conditions, including the absence of a comprehensive digital governance law, fragmented institutional responsibilities, accumulated negative user experiences with digital services, digital inequality, and disparities in digital literacy and legal awareness. Furthermore, economic constraints, international sanctions, and rapid technological changes have intensified the complexity of trust-building efforts within the Iranian digital ecosystem.

1.4 Research Gap and Contribution

A review of the existing literature reveals that most previous studies have examined digital trust as an antecedent or consequence of technology adoption, e-government acceptance, e-commerce behavior, or online consumer trust. Although these studies provide valuable insights, they rarely address digital trust as a comprehensive governance phenomenon encompassing legal, institutional, technological, economic, and socio-cultural dimensions simultaneously. Moreover, little attention has been paid to developing context-specific frameworks that explain how digital trust is formed, maintained, and institutionalized in developing countries, particularly in relation to emerging immersive digital environments.

The present study seeks to address these gaps by developing and validating an indigenous digital trust model tailored to the Iranian context, while also considering the implications for trust in metaverse and virtual environments. Using an exploratory sequential mixed-methods design, the study integrates grounded theory and Partial Least Squares Structural Equation Modeling (PLS-SEM) to identify the causal conditions, contextual factors, intervening conditions, strategic responses, and consequences associated with digital trust. In addition, the study proposes an operational roadmap and a policy–action matrix to facilitate practical implementation of digital trust strategies at the national level.

This research contributes to the literature in four significant ways. First, it extends existing digital trust theories by incorporating context-specific institutional and legal determinants relevant to developing countries. Second, it conceptualizes digital trust as a governance-centered phenomenon rather than merely a technological or behavioral construct. Third, it provides a practical implementation framework that bridges the gap between theoretical

models and policymaking processes. Fourth, it positions the governance-centered trust framework within the emerging discourse on trust in immersive digital ecosystems, including the metaverse and virtual platforms. Collectively, these contributions offer new insights for scholars, policymakers, and practitioners seeking to promote trustworthy digital ecosystems in Iran and other emerging digital societies.

Literature Review

2.1 Theoretical Foundations of Digital Trust

Trust has long been recognized as a fundamental concept in social sciences, organizational studies, and governance research. Classical scholars such as Luhmann (1979) conceptualized trust as a mechanism for reducing complexity and uncertainty in social interactions. In digital environments, where interactions increasingly occur through technological systems rather than direct interpersonal relationships, trust assumes new forms and functions.

Digital trust is generally defined as stakeholders' confidence in the integrity, reliability, security, transparency, and accountability of digital technologies and institutions. Unlike traditional trust, which is often built through direct interpersonal interactions and repeated social exchanges, digital trust is predominantly system-oriented and relies on users' perceptions of technological and institutional reliability. Consequently, digital trust emerges at the intersection of technology, governance, law, and social expectations.

Recent studies suggest that digital trust is becoming an essential prerequisite for digital transformation initiatives. Citizens are more likely to adopt digital services when they perceive that their personal information is protected, institutional actors are accountable, and digital systems operate fairly and transparently. Conversely, trust deficiencies may result in resistance to technological innovations, reduced participation in digital services, and lower effectiveness of digital governance programs.

The literature commonly identifies five major dimensions of digital trust: (1) security and cybersecurity protection, (2) privacy and personal data protection, (3) transparency and explainability of digital processes, (4) accountability and institutional responsibility, and (5) ethical and fair use of digital technologies. Together, these dimensions' shape users' perceptions of trustworthiness and influence their willingness to engage with digital ecosystems.

2.2 Trust in Immersive Environments and the Metaverse

The emergence of immersive digital environments has expanded the conceptual boundaries of digital trust. In virtual worlds and metaverse platforms, trust relationships become more complex due to the convergence of physical and digital identities, the persistence of virtual assets, and the governance authority of platform operators (Shin, 2022; Wang et al., 2023).

Dwivedi et al. (2022) identify several trust-related challenges in the metaverse, including identity verification, data provenance, content moderation, algorithmic transparency, and the enforcement of cross-jurisdictional regulations. Similarly, Tan and Salo (2023) highlight that trust in virtual environments is shaped by factors such as avatar authenticity, social presence, platform reputation, and the perceived fairness of governance mechanisms. Kitsios and Kamariotou (2023) argue that digital transformation initiatives in immersive environments require a rethinking of trust-building strategies, as traditional institutional trust mechanisms may not translate directly to virtual contexts.

Lee et al. (2021) and Mystakidis (2022) emphasize the importance of decentralized governance models, user empowerment, and transparent algorithmic processes in fostering trust in metaverse ecosystems. The ISACA Digital Trust Ecosystem Framework (2024) has been extended to include immersive environments, recognizing that trust in virtual worlds requires attention to technical, organizational, and human dimensions simultaneously.

These studies underscore that trust in emerging digital environments is not merely a technological issue but a governance challenge that requires coordinated legal, institutional,

and technical interventions. The governance-centered perspective adopted in this study aligns with this broader understanding, offering a framework that can potentially inform trust-building strategies in both conventional and immersive digital ecosystems.

2.3 International Frameworks of Digital Trust

Over the last decade, several international organizations have proposed conceptual and operational frameworks for understanding digital trust.

World Economic Forum (WEF) – The WEF (2024) conceptualizes digital trust as the outcome of interactions among technology, governance, and ethics. Its framework emphasizes cybersecurity, privacy protection, transparency, accountability, and responsible technology use as the fundamental pillars of trustworthy digital ecosystems.

European Union Framework – The European Union has approached digital trust primarily through regulatory mechanisms, particularly the General Data Protection Regulation (GDPR). This framework emphasizes individual rights, organizational accountability, lawful data processing, and independent regulatory oversight. The European model treats trust as a consequence of robust institutional and legal safeguards.

NIST Framework – The National Institute of Standards and Technology (NIST) focuses primarily on cybersecurity risk management and privacy engineering. In this perspective, trust emerges from organizations' ability to identify, assess, and mitigate digital risks while maintaining system resilience and operational continuity.

ISACA Digital Trust Ecosystem Framework – ISACA (2024) proposes a multidimensional ecosystem approach, integrating technological, organizational, and human dimensions. Unlike purely technical perspectives, this framework recognizes that trust depends on governance processes, organizational culture, stakeholder relationships, and technological capabilities simultaneously.

Although these frameworks differ in emphasis, they share a common assumption: digital trust is not merely a technological issue but a multidimensional governance challenge requiring coordinated legal, institutional, and technical interventions.

2.4 Digital Trust in Developing Countries

While digital trust has received substantial attention in developed economies, its dynamics in developing countries remain less understood. Existing evidence suggests that institutional quality, governance effectiveness, social capital, economic stability, and cultural norms significantly influence trust formation in digital environments (Almarashdah et al., 2024; Beyene et al., 2024).

Developing countries often face additional barriers, including fragmented governance structures, weak regulatory frameworks, limited enforcement capacity, unequal access to digital infrastructure, and lower levels of institutional trust (Ibor et al., 2025; Ofosu-Mensah Ababio & Yiadom, 2024). Consequently, trust-building mechanisms that are effective in highly institutionalized contexts may not necessarily produce similar outcomes in developing societies (Nosike, 2024; Raheem et al., 2024).

Recent studies in emerging economies have highlighted the importance of contextualizing digital trust models according to local governance arrangements and socio-cultural conditions. Nevertheless, most existing research continues to rely on theoretical assumptions and measurement frameworks originally developed in Western contexts.

2.5 Digital Trust Research in Iran

Research related to digital trust in Iran has expanded in recent years, particularly in the domains of e-government, e-commerce, digital platforms, and online consumer behavior. Previous studies have examined topics such as electronic trust in government services, consumer trust in digital marketplaces, cultural determinants of online trust, and opportunities and challenges of digital governance.

These studies have generated valuable insights regarding specific dimensions of trust. However, the majority of them exhibit three major limitations. First, digital trust is typically examined as an independent or mediating variable influencing technology adoption rather than as a comprehensive governance phenomenon. Second, most studies focus on specific sectors such as e-commerce, cryptocurrency transactions, or electronic government services, limiting their ability to explain trust formation at the broader national governance level. Third, existing studies rarely integrate legal, institutional, technological, economic, cultural, and media-related factors within a single analytical framework. As a result, the broader mechanisms through which digital trust is created, maintained, and institutionalized within Iran's digital ecosystem remain insufficiently understood.

2.6 Research Gap

The review of international and domestic literature reveals several important gaps. First, existing digital trust studies predominantly emphasize technological and behavioral factors while paying limited attention to governance-related determinants such as institutional fragmentation, regulatory deficiencies, and policy coordination. Second, current frameworks have largely been developed in advanced economies characterized by mature legal systems, strong institutional capacities, and relatively high levels of social trust. Consequently, their explanatory power may be limited in developing countries with different governance structures and socio-political conditions. Third, previous studies have rarely employed a comprehensive paradigmatic perspective that simultaneously incorporates causal conditions, contextual factors, intervening conditions, strategic responses, and governance outcomes. Fourth, little attention has been devoted to translating theoretical trust models into actionable policy instruments. To the best of the authors' knowledge, no previous study has proposed an operational roadmap and policy–action matrix for implementing digital trust at the national governance level. Fifth, the relationship between digital trust and emerging immersive environments, including the metaverse, has received limited empirical attention in developing-country contexts.

Therefore, this study addresses a significant theoretical and practical gap by developing and validating an indigenous governance-centered digital trust model tailored to Iran's institutional, legal, technological, economic, and socio-cultural context, while also positioning this framework within the broader discourse on trust in immersive digital ecosystems. Furthermore, the study extends existing digital trust literature by offering a practical implementation framework that supports evidence-based policymaking and strategic governance reform.

Method

3.1 Research Design

This study employed an exploratory sequential mixed-methods design to develop and validate an indigenous digital trust model for Iran. The mixed-methods approach was selected because digital trust is a multidimensional and context-dependent phenomenon that requires both qualitative exploration and quantitative validation.

The research was conducted in two consecutive phases. In the first phase, grounded theory methodology (Strauss & Corbin, 1998) was applied to identify the underlying dimensions, conditions, strategies, and consequences of digital trust within the Iranian context. Data analysis was performed using MAXQDA software to facilitate systematic coding and category development. In the second phase, the conceptual model emerging from the qualitative findings was empirically validated using Partial Least Squares Structural Equation Modeling (PLS-SEM) through Smart PLS 3 software. The integration of qualitative and quantitative methods enabled the study to generate a context-specific theoretical framework while simultaneously assessing its empirical validity.

3.2 Qualitative Phase

3.2.1 Participants and Sampling

The qualitative phase involved experts with extensive experience in information technology, digital governance, cybersecurity, digital platforms, technology law, and public policy. Participants were selected through purposive theoretical sampling to ensure rich and relevant insights regarding digital trust. Snowball sampling was additionally employed, with initial participants recommending other qualified experts.

The inclusion criteria required participants to possess: (1) a minimum of five years of professional experience in digital governance or information technology; (2) direct involvement in policymaking, digital platform management, cybersecurity, technology regulation, or academic research; and (3) familiarity with digital transformation initiatives and governance challenges in Iran.

A total of 12 experts participated in the interviews. Theoretical saturation was reached after the eighth interview; however, four additional interviews were conducted to enhance theoretical robustness and confirm emerging categories.

3.2.2 Data Collection

Data were collected through semi-structured interviews conducted between 2024 and 2025. The interview protocol was designed to explore participants' perceptions and experiences regarding trust-building mechanisms in digital environments. Key interview topics included: drivers and barriers of digital trust; institutional and regulatory challenges; citizens' experiences with digital services; digital governance structures; trust-enhancing strategies and policy interventions; expected outcomes of improved digital trust; and, where relevant, perceptions of trust in emerging virtual and immersive platforms.

Each interview lasted approximately 45–90 minutes and was audio-recorded with participants' consent. In addition to interviews, supplementary data were obtained from policy documents, official reports, digital governance regulations, and field notes to strengthen data triangulation.

3.2.3 Data Analysis

Qualitative data were analyzed following Strauss and Corbin's (1998) grounded theory procedures.

Open Coding: Interview transcripts were examined line by line to identify meaningful concepts and initial codes. This process resulted in the extraction of 74 primary concepts reflecting participants' perceptions and experiences regarding digital trust.

Axial Coding: The identified concepts were systematically grouped into categories and subcategories. Relationships among categories were then established using the Strauss–Corbin paradigm model, which links causal conditions, contextual conditions, intervening conditions, strategies, and consequences.

Selective Coding: During the final stage, the core category was identified and integrated with all other categories. The central phenomenon emerging from the data was labeled Governance-Centered Digital Trust, representing the focal concept around which the entire theoretical model was constructed.

The final qualitative model consisted of six major categories and twenty-four subcategories. Table 1 presents a summary of the coding process.

Table 1. Summary of Open, Axial, and Selective Coding

Coding Stage	Output	Example
Open Coding	74 initial concepts	"Lack of data protection law", "Fragmented institutional responsibilities", "Negative past experiences", "Digital divide", "Low legal awareness"
Axial Coding	24 subcategories	"Legal deficiencies", "Institutional fragmentation", "User dissatisfaction", "Access inequality", "Knowledge gap"
Selective Coding	6 major categories	Causal Conditions, Central Phenomenon, Contextual Conditions, Intervening Conditions, Strategies, Consequences

3.2.4 Trustworthiness of Qualitative Findings

To enhance the credibility and trustworthiness of the qualitative findings, several procedures were implemented: (1) data triangulation through interviews, documents, and field observations; (2) member checking with selected participants; (3) prolonged engagement with the data; (4) peer review and expert evaluation; and (5) continuous comparison of emerging concepts and categories. These measures increased the reliability, consistency, and interpretive validity of the grounded theory model.

3.3 Quantitative Phase

3.3.1 Instrument Development

A researcher-developed questionnaire was constructed based on the categories identified during the qualitative phase. The questionnaire consisted of 28 measurement items distributed across six latent constructs: Causal Conditions (5 items), Central Phenomenon (4 items), Contextual Conditions (3 items), Intervening Conditions (3 items), Strategies (5 items), and Consequences (8 items). Responses were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

Content validity was assessed by a panel of five academic and professional experts specializing in information systems, digital governance, and research methodology.

3.3.2 Population and Sample

The target population consisted of managers, experts, and professionals working in the fields of information technology and digital governance in Iran. A convenience sampling approach was employed due to the specialized nature of the target respondents.

The sample size of 100 valid questionnaires was justified based on the **10-times rule** for PLS-SEM (Hair et al., 2022), which recommends that the sample size should be at least ten times the largest number of structural paths directed at a particular construct in the model. In this study, the maximum number of paths directed at any construct was five, yielding a minimum required sample size of 50. The achieved sample of 100 exceeded this requirement, ensuring adequate statistical power.

3.3.3 Reliability Assessment

Internal consistency reliability was evaluated using Cronbach's Alpha and Composite Reliability (CR). Cronbach's Alpha values ranged between 0.748 and 0.822, exceeding the minimum acceptable threshold of 0.70. Similarly, all Composite Reliability values exceeded the recommended value of 0.70, indicating satisfactory reliability of the measurement model.

3.4 Structural Equation Modeling

3.4.1 Analytical Approach

The conceptual framework was validated using Partial Least Squares Structural Equation Modeling (PLS-SEM) through SmartPLS 3 software. PLS-SEM was selected for three reasons: (1) the exploratory nature of the research; (2) the relatively small sample size; and (3) the non-normal distribution of the data. The Kolmogorov–Smirnov test indicated deviations from normality, supporting the use of variance-based structural equation modeling techniques.

3.4.2 Measurement Model Evaluation

The measurement model was assessed using the following criteria: indicator loadings, Composite Reliability (CR), Average Variance Extracted (AVE), and discriminant validity using the Fornell–Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio. The results demonstrated that all factor loadings exceeded the recommended threshold of 0.40 and were statistically significant. All AVE values were greater than 0.50, confirming convergent validity. The Fornell–Larcker criterion and HTMT values supported discriminant validity among the constructs.

3.4.3 Structural Model Evaluation

The structural model was evaluated by examining path coefficients (β), t-values obtained through bootstrapping (5,000 subsamples), statistical significance levels, R^2 values, Q^2 values (Stone-Geisser), and the overall model fit (SRMR and GOF).

All hypothesized relationships were statistically significant at the 0.05 significance level. The model achieved a Goodness-of-Fit (GOF) value of 0.601, substantially exceeding the recommended threshold of 0.36, indicating strong explanatory power and satisfactory model fit. The Standardized Root Mean Square Residual (SRMR) was 0.058, below the recommended threshold of 0.08, further confirming acceptable model fit.

3.5 Ethical Considerations

Participation in the study was voluntary, and informed consent was obtained from all interviewees and survey respondents. Participants were assured that their identities and responses would remain confidential and would be used exclusively for academic purposes. All research procedures complied with accepted ethical standards for social science research.

Findings

4.1 Qualitative Findings: Development of the Indigenous Digital Trust Model

The qualitative analysis generated a comprehensive conceptual framework explaining the formation and development of digital trust within Iran's digital governance ecosystem. Through open coding, 74 initial concepts were identified from the interview transcripts. These concepts were subsequently consolidated into 24 subcategories and six major categories through axial and selective coding procedures.

The resulting paradigm model was organized around a central phenomenon labeled Governance-Centered Digital Trust, which emerged as the core explanatory concept linking all other categories.

4.1.1 Causal Conditions

The analysis revealed five major causal conditions influencing digital trust in Iran: (1) digital legal and regulatory deficiencies; (2) institutional fragmentation in digital policymaking; (3) citizens' accumulated negative experiences with digital services; (4) digital divide and unequal access to technological infrastructure; and (5) insufficient development of digital literacy and legal awareness.

Among these factors, the absence of a comprehensive legal framework for data protection and digital governance was repeatedly identified as the most significant barrier to trust formation. Participants emphasized that uncertainty regarding data ownership, privacy protection, and institutional accountability creates persistent concerns among citizens and businesses, thereby weakening confidence in digital systems.

"One of the interviewees stated: «The absence of a comprehensive personal data protection law is the biggest obstacle to citizens' trust in digital systems in Iran. People do not know where and how their information is being used»" (Expert 3).

"Another participant emphasized: «The lack of legal clarity regarding digital rights and data governance creates a situation of perpetual uncertainty. Businesses are hesitant to invest in digital platforms, and citizens are reluctant to share their personal information»" (Expert 8).

4.1.2 Central Phenomenon: Governance-Centered Digital Trust

The core category emerging from the analysis was governance-centered digital trust. Participants described digital trust as a multidimensional belief that digital institutions possess the capability and willingness to protect personal data, ensure transparency, provide accountability, and respond effectively to failures or violations. Unlike technology-centered perspectives, respondents consistently emphasized that trust is fundamentally linked to governance quality rather than technological sophistication alone.

"Expert 5 explained: «Digital trust is not about having the most advanced technology; it's about whether citizens believe that the institutions behind the technology are trustworthy. When people trust the government's intentions and capabilities, they will use digital services even with basic infrastructure.»"

"Another participant noted: «In Iran, the governance dimension is the most critical factor. People may have access to sophisticated digital platforms, but if they don't trust the institutions managing them, they will not engage»" (Expert 10).

4.1.3 Contextual Conditions

Three contextual factors were found to shape the environment in which digital trust develops: (1) social capital and institutional trust; (2) public attitudes toward technology; and (3) the status of national information infrastructure and access to the global Internet. Interviewees highlighted that digital trust cannot be isolated from broader societal trust patterns. Low levels of institutional trust in offline environments frequently transfer into digital interactions.

"Expert 2 observed: «Trust in digital services is a reflection of trust in society as a whole. If people do not trust government institutions offline, they will not trust them online either. This is a fundamental challenge that cannot be solved through technology alone.»"

4.1.4 Intervening Conditions

Three major intervening conditions were identified: (1) global digital transformations and technological developments; (2) economic conditions and business environment constraints; and (3) media influence and public perception. Participants noted that international sanctions, technological dependency, and rapidly evolving digital standards significantly affect trust dynamics within the Iranian context. Similarly, media narratives were found to play a critical role in shaping public perceptions of digital risks and opportunities.

"Expert 7 commented: «International sanctions have significantly affected Iran's digital infrastructure. The inability to access advanced technologies and international platforms creates a sense of technological isolation that undermines trust in domestically developed digital services.»"

"Expert 11 added: «Media coverage of cybersecurity incidents and data breaches has a powerful impact on public perception. Each reported incident reinforces the narrative that digital services are unsafe.»"

4.1.5 Strategic Responses

Six strategic categories emerged as essential mechanisms for strengthening digital trust: (1) institutionalization of a comprehensive digital governance law; (2) effective enforcement mechanisms; (3) institutional integration and coordination; (4) transparency, accountability, and responsiveness; (5) strengthening cybersecurity architecture and resilience; and (6) enhancing public digital literacy and awareness. These strategies collectively constitute the primary governance mechanisms through which trust can be systematically cultivated and sustained.

"Expert 4 emphasized: «Without a unified legal framework, all other efforts are fragmented. We need a comprehensive digital governance law that clearly defines citizens' rights and institutional responsibilities.»"

"Expert 12 stated: «Transparency is the key. When citizens can see how their data is being used and have mechanisms to hold institutions accountable, trust gradually increases.»"

4.1.6 Consequences

The implementation of trust-enhancing strategies was associated with several expected outcomes: (1) advancement toward digital governance maturity; (2) strengthening digital trust as a strategic governance asset; (3) increased social capital and public trust; (4) greater citizen participation and digital rights awareness; (5) higher adoption of digital services; (6)

improved integration into global digital ecosystems; (7) enhanced productivity and economic growth. These findings suggest that digital trust functions not only as a governance objective but also as a catalyst for broader social and economic development.

4.1.7 Paradigmatic Model of Governance-Centered Digital Trust

Based on the Strauss and Corbin grounded theory paradigm, the findings were integrated into a comprehensive paradigmatic model explaining the formation and development of digital trust within Iran's digital ecosystem. The core phenomenon emerging from the qualitative analysis was Governance-Centered Digital Trust, representing stakeholders' confidence in the capability, accountability, transparency, and responsiveness of digital institutions.

The paradigm model consists of six interrelated components:

Causal Conditions: The emergence of governance-centered digital trust is influenced by several causal factors, including: (1) legal and regulatory deficiencies in the digital domain, (2) institutional fragmentation in digital policymaking, (3) accumulated negative citizen experiences with digital services, (4) digital inequality and unequal access to infrastructure, and (5) insufficient digital literacy and digital rights awareness.

Central Phenomenon: The central phenomenon is governance-centered digital trust, defined as citizens' and stakeholders' belief that digital institutions possess both the capacity and commitment to protect personal data, ensure transparency, provide accountability, and effectively address failures and violations.

Contextual Conditions: The development of digital trust occurs within a broader socio-institutional environment shaped by social capital and institutional trust, public attitudes toward technology, and the quality of national digital infrastructure and Internet accessibility.

Intervening Conditions: The effectiveness of trust-building processes is influenced by intervening factors such as global technological developments, economic conditions and business constraints, and media influence on public perceptions of digital opportunities and risks.

Strategies: To strengthen digital trust, the model identifies six strategic responses: (1) establishment of a comprehensive digital governance law, (2) effective regulatory enforcement mechanisms, (3) institutional integration and policy coordination, (4) enhancement of transparency, accountability, and responsiveness, (5) strengthening cybersecurity resilience, and (6) promotion of public digital literacy and digital rights awareness.

Consequences: Implementation of these strategies leads to several positive outcomes, including increased digital governance maturity, stronger digital trust, enhanced social capital, greater citizen participation, higher adoption of digital services, improved integration into global digital ecosystems, and sustainable economic growth.

Figure 1 illustrates the paradigmatic model and demonstrates how causal conditions shape governance-centered digital trust, which, under specific contextual and intervening conditions, leads to the adoption of strategic responses and ultimately generates governance, social, and economic outcomes.

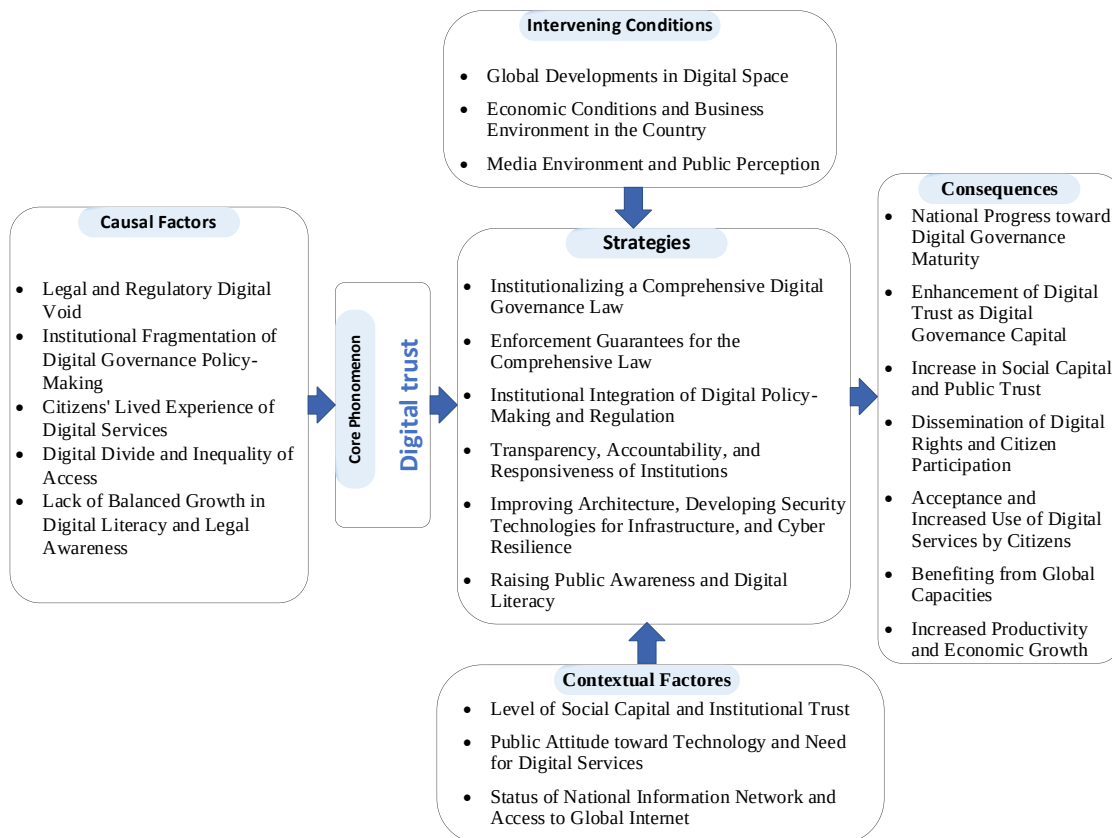


Figure 1. illustrates the paradigmatic model

4.2 Indigenous Characteristics of the Proposed Model

The findings indicate that the proposed framework contains several context-specific characteristics that distinguish it from existing international models. First, legal and regulatory deficiencies emerged as a primary causal factor rather than a contextual variable. Second, institutional fragmentation was identified as a structural obstacle that directly undermines citizens' trust in digital governance arrangements. Third, participants emphasized the importance of accumulated negative user experiences, a dimension that has received relatively limited attention in international digital trust frameworks. Furthermore, the findings revealed the importance of distinguishing between digital literacy and digital rights awareness. While many citizens possess basic technological competencies, awareness of legal rights and digital protection mechanisms remains limited. These characteristics collectively underscore the necessity of developing context-sensitive digital trust frameworks for developing countries.

4.3 Quantitative Findings

4.3.1 Measurement Model Assessment

The measurement model was evaluated through reliability and validity analyses. All factor loadings exceeded the minimum acceptable threshold and were statistically significant. Composite Reliability (CR) values ranged from 0.736 to 0.886, demonstrating satisfactory internal consistency. Similarly, Average Variance Extracted (AVE) values ranged from 0.562 to 0.663, exceeding the recommended threshold of 0.50 and confirming convergent validity.

The Fornell–Larcker criterion further confirmed discriminant validity among all latent constructs. Additionally, the Heterotrait-Monotrait (HTMT) ratios were all below the recommended threshold of 0.85, further confirming discriminant validity.

Table 2. Reliability and Convergent Validity Assessment

Construct	Cronbach's Alpha	CR	AVE
Causal Conditions	0.782	0.757	0.592
Central Phenomenon	0.748	0.736	0.658
Contextual Conditions	0.811	0.808	0.663
Intervening Conditions	0.769	0.787	0.584
Strategies	0.822	0.836	0.562
Consequences	0.796	0.886	0.639

The results indicate acceptable reliability and validity across all constructs.

Table 3. Fornell–Larcker Discriminant Validity Assessment

Construct	Causal	Central	Contextual	Intervening	Strategies	Consequences
Causal	0.769					
Central	0.538	0.811				
Contextual	0.412	0.483	0.814			
Intervening	0.398	0.716	0.527	0.764		
Strategies	0.451	0.751	0.483	0.716	0.750	
Consequences	0.427	0.639	0.394	0.528	0.557	0.799

Note: Diagonal values (bold) represent the square root of AVE. Off-diagonal values represent construct correlations. For adequate discriminant validity, diagonal values should exceed off-diagonal values in the corresponding rows and columns.

4.3.2 Structural Model Assessment

The structural model was assessed through path coefficient analysis and bootstrapping procedures (5,000 subsamples). All hypothesized relationships were statistically significant at the 95% confidence level.

The strongest relationship was observed between the central phenomenon and strategic responses ($\beta = 0.751$, $t = 3.248$, $p < 0.01$), suggesting that governance-centered digital trust serves as a critical driver of institutional and policy interventions. The influence of causal conditions on digital trust was also substantial ($\beta = 0.538$, $t = 4.254$, $p < 0.001$), indicating the importance of addressing legal, institutional, and experiential barriers.

Table 4. Structural Model Results

Hypothesized Path	β	t-value	p-value	Result
Causal Conditions → Central Phenomenon	0.538	4.254	0.001	Supported
Central Phenomenon → Strategies	0.751	3.248	0.005	Supported
Contextual Conditions → Strategies	0.483	2.465	0.014	Supported
Intervening Conditions → Strategies	0.716	2.417	0.016	Supported
Strategies → Consequences	0.557	2.661	0.008	Supported

The findings confirm that digital trust is influenced by a complex interaction of structural, contextual, and environmental factors and that trust-enhancing strategies significantly contribute to governance and societal outcomes.

4.3.3 Model Fit and Predictive Relevance

The overall goodness-of-fit (GOF) value of the structural model was calculated as 0.601. This value substantially exceeds the recommended benchmark of 0.36, indicating a strong overall fit and substantial explanatory power.

Table 5. R^2 and Q^2 Values

Construct	R^2	Q^2
Central Phenomenon	0.538	0.342
Strategies	0.681	0.415
Consequences	0.557	0.328

The R^2 values indicate that causal conditions explain 53.8% of the variance in the central phenomenon, while the model explains 68.1% of the variance in strategies and 55.7% of the variance in consequences. The Q^2 values, all exceeding zero, confirm the predictive relevance of the model. The Standardized Root Mean Square Residual (SRMR) was 0.058, below the recommended threshold of 0.08, confirming acceptable model fit.

The quantitative findings therefore provide empirical support for the conceptual framework developed during the qualitative phase and validate the proposed indigenous digital trust model for Iran.

Discussion

5.1 *Interpreting the Findings in the Context of Digital Trust Theory*

This study aimed to develop and validate an indigenous digital trust model tailored to the Iranian context. The findings demonstrate that digital trust should be understood as a multidimensional governance phenomenon rather than merely a technological or cybersecurity-related issue. The proposed framework identifies legal, institutional, technological, economic, cultural, and media-related factors as interconnected components influencing the formation and sustainability of digital trust.

The qualitative and quantitative findings collectively indicate that trust in digital environments is fundamentally shaped by governance structures and institutional arrangements. This result challenges purely technology-centered approaches that equate digital trust with cybersecurity capabilities or technical performance. Instead, the study suggests that technological reliability constitutes only one component of a broader trust ecosystem.

The identification of governance-centered digital trust as the core category highlights the importance of institutional legitimacy, regulatory effectiveness, and accountability mechanisms in fostering citizens' confidence in digital systems. This finding is consistent with contemporary digital governance literature, which increasingly emphasizes the role of institutional quality in shaping public trust toward digital transformation initiatives (Mazhar et al., 2025; Vial, 2023).

5.2 *Comparison with International Digital Trust Frameworks*

The findings exhibit substantial convergence with major international digital trust frameworks while simultaneously revealing important contextual differences.

Consistent with the World Economic Forum framework (WEF, 2024), participants emphasized cybersecurity, transparency, accountability, and responsible governance as essential foundations of digital trust. Similarly, the importance of privacy protection and legal safeguards aligns with the principles underlying the European Union's GDPR framework. However, the findings extend existing frameworks by identifying institutional fragmentation and regulatory inconsistency as primary trust barriers. While most international models assume relatively stable institutional environments, the Iranian context demonstrates that trust deficits may originate from fragmented governance arrangements and overlapping regulatory responsibilities.

Likewise, the ISACA Digital Trust Ecosystem Framework (2024) emphasizes interactions among technological, organizational, and human dimensions. The present study supports this perspective but further demonstrates that governance capacity acts as a mediating mechanism connecting these dimensions within developing-country contexts.

A notable extension of this study is its consideration of trust in immersive digital environments. While international frameworks have begun to address metaverse-related trust challenges (Shin, 2022; Wang et al., 2023), the present study's governance-centered approach offers a complementary perspective. The findings suggest that the governance mechanisms identified—legal clarity, institutional coordination, transparency, and accountability—are equally relevant for trust-building in virtual worlds, where platform governance and algorithmic accountability are emerging as critical concerns (Kitsios & Kamariotou, 2023; Tan & Salo, 2023). This suggests that the governance-centered framework may serve as a foundation for developing trust strategies in both conventional and immersive digital ecosystems.

Therefore, although international frameworks provide valuable foundations, their direct application may be insufficient in countries characterized by institutional complexity, evolving regulatory environments, and lower levels of institutional trust.

5.3 *Institutional Trust and Digital Trust*

One of the most significant findings concerns the relationship between institutional trust and digital trust. The results indicate that citizens frequently transfer perceptions formed in

offline institutional environments into digital interactions. Consequently, digital trust cannot be isolated from broader governance realities.

This finding supports Institutional Trust Theory, which argues that confidence in institutions is a prerequisite for confidence in institutional outputs and services (Mayer et al., 1995). In contexts where institutional trust is limited, even technologically advanced digital services may encounter adoption barriers. The results suggest that strengthening digital trust requires simultaneous improvements in governance quality, transparency, responsiveness, and institutional accountability. Investments in digital infrastructure alone are unlikely to produce sustainable trust gains unless accompanied by governance reforms.

The path coefficient between causal conditions and the central phenomenon ($\beta = 0.538$) provides empirical support for this argument. This relatively strong relationship indicates that addressing legal deficiencies and institutional fragmentation should be prioritized alongside technological investments.

5.4 Path Dependence and the Role of Negative Experiences

Another important contribution of the study concerns the role of accumulated negative experiences with digital services. Participants repeatedly highlighted previous encounters with service interruptions, system failures, poor user experiences, and inadequate institutional responses as sources of persistent distrust. These experiences influence future perceptions and behaviors, even when technological improvements are introduced.

This finding supports Path Dependence Theory, which argues that historical experiences shape future decision-making trajectories. In the context of digital governance, trust appears to evolve cumulatively, meaning that past failures continue to influence contemporary trust judgments. The implication is that trust recovery may require considerably greater effort than trust creation. Policymakers and digital service providers must therefore recognize that rebuilding trust involves not only technical improvements but also visible accountability and corrective action mechanisms.

5.5 Reconsidering Diffusion of Innovation Theory

The findings also contribute to the literature on technology adoption and innovation diffusion. According to Rogers' Diffusion of Innovation Theory (2003), adoption is primarily influenced by perceived relative advantage, compatibility, complexity, trialability, and observability. While these factors remain important, the present study suggests that trust may function as a prerequisite condition for adoption in governance contexts.

Participants frequently reported that citizens may avoid digital services despite recognizing their functional benefits if they lack confidence in the institutions providing them. This observation indicates that, in developing countries with institutional challenges, trust may exert a stronger influence on digital adoption than perceived technological advantages. Consequently, digital trust should be considered an essential antecedent within future digital adoption models, particularly in contexts of institutional fragility.

5.6 Theoretical Contributions

This study contributes to digital trust literature in several important ways. First, it introduces a governance-centered conceptualization of digital trust that integrates legal, institutional, technological, economic, and socio-cultural dimensions within a single analytical framework. Second, it extends existing digital trust theories by identifying digital legal deficiencies and institutional fragmentation as independent causal conditions rather than secondary contextual variables. Third, the study highlights the importance of accumulated negative user experiences as a distinct trust determinant, thereby enriching current understandings of trust formation processes. Fourth, the research distinguishes between digital literacy and digital rights awareness, demonstrating that technological competence alone is insufficient for sustainable trust development. Fifth, the study contributes methodologically by integrating grounded theory and structural equation modeling to

develop and validate a context-sensitive digital trust framework. Sixth, by situating the governance-centered framework within the broader discourse on trust in immersive digital environments, the study opens avenues for future research on trust in metaverse and virtual platforms, suggesting that the governance mechanisms identified here may have relevance beyond conventional digital contexts.

5.7 Practical and Policy Implications

The findings have important implications for policymakers, regulators, and digital service providers. At the national level, the results suggest that comprehensive digital governance legislation should be prioritized as a foundational trust-building mechanism. Regulatory clarity regarding data protection, privacy rights, platform accountability, and institutional responsibilities can significantly reduce uncertainty among citizens and organizations.

Furthermore, the findings highlight the need for greater institutional coordination. Establishing integrated governance structures and reducing regulatory fragmentation may improve policy consistency and strengthen public confidence. The study also emphasizes the importance of transparency and accountability mechanisms. Public reporting systems, algorithmic transparency initiatives, and accessible complaint-resolution procedures can increase perceptions of institutional responsiveness.

For digital service providers, the results underscore the strategic importance of user experience, cybersecurity certification, incident disclosure practices, and rapid response mechanisms. Trust should be treated as a strategic organizational asset rather than merely a compliance requirement. Finally, investments in digital literacy programs should be complemented by initiatives that increase citizens' awareness of digital rights, privacy protections, and available redress mechanisms.

5.8 Implications for Developing Countries and Immersive Environments

Although the proposed framework was developed specifically for Iran, several findings may be relevant to other developing countries and to the emerging discourse on trust in immersive digital environments. Many emerging economies face similar challenges, including fragmented governance structures, evolving legal systems, digital inequalities, and fluctuating levels of institutional trust. Consequently, the framework may offer a useful foundation for comparative studies examining digital trust formation across different socio-political contexts.

Moreover, as immersive digital environments become more prevalent, the governance-centered approach offers insights into trust-building in virtual worlds. The emphasis on institutional legitimacy, transparency, and accountability applies equally to platform governance in metaverse ecosystems, where trust in platform operators and algorithmic processes is critical for user engagement (Dwivedi et al., 2022; Shin, 2022). The framework's attention to legal clarity and user rights may also inform the development of regulatory approaches to virtual asset protection, identity verification, and cross-border data flows in immersive environments.

However, the findings also reinforce the importance of contextual adaptation. Effective digital trust strategies must reflect local governance arrangements, cultural characteristics, and institutional realities rather than relying exclusively on imported policy models. Overall, the study suggests that successful digital transformation depends not only on technological advancement but also on the development of trustworthy governance ecosystems capable of sustaining long-term public confidence.

Conclusion

6.1 Conclusion

Digital trust has emerged as a fundamental prerequisite for digital transformation, digital governance, and sustainable digital economic development. Despite its growing importance, existing digital trust frameworks have been predominantly developed within the institutional and socio-economic contexts of developed countries, limiting their applicability to developing nations. This study addressed this gap by developing and validating an indigenous digital trust model tailored to the Iranian context, while also positioning the framework within the broader discourse on trust in emerging immersive digital environments, including the metaverse and virtual platforms.

Using an exploratory sequential mixed-methods design, the study integrated grounded theory (Strauss & Corbin, 1998) and Partial Least Squares Structural Equation Modeling (PLS-SEM) to identify and validate the key determinants, mechanisms, and outcomes of digital trust. The qualitative phase involved semi-structured interviews with 12 experts selected through purposive and snowball sampling, with data analyzed using MAXQDA through open, axial, and selective coding. The quantitative phase employed a researcher-developed questionnaire administered to 100 IT managers and professionals, with data analyzed using SmartPLS 3.

The findings revealed that governance-centered digital trust constitutes the core phenomenon shaping trust formation in Iran's digital ecosystem. Legal and regulatory deficiencies, institutional fragmentation, digital inequalities, insufficient digital rights awareness, and accumulated negative user experiences were identified as major barriers to trust development. Conversely, regulatory reform, institutional coordination, cybersecurity resilience, transparency, accountability, and digital literacy enhancement emerged as critical trust-building strategies.

The validated framework demonstrates that digital trust is not merely a technological issue but a multidimensional governance construct influenced by legal, institutional, technological, economic, and socio-cultural factors. The path analysis confirmed significant relationships among all constructs, with the model explaining 68.1% of the variance in trust-building strategies and achieving strong overall fit ($GOF = 0.601$, $SRMR = 0.058$). The findings further indicate that strengthening digital trust can generate broader societal benefits, including increased adoption of digital services, enhanced citizen participation, improved governance effectiveness, and greater integration into the global digital economy.

6.2 Theoretical Implications

This study makes several important contributions to the digital trust and digital governance literature. First, it advances existing knowledge by conceptualizing digital trust as a governance-centered phenomenon rather than a purely technological or behavioral construct. This perspective broadens the analytical scope of digital trust research and highlights the central role of governance quality in trust formation.

Second, the study extends current theoretical frameworks by identifying institutional fragmentation and digital legal deficiencies as primary causal determinants of digital trust in developing-country contexts. These findings suggest that governance structures and regulatory coherence are as important as technological capabilities in shaping trust outcomes. Third, the research contributes to trust theory by demonstrating the long-term influence of accumulated negative digital experiences on citizens' trust perceptions. This finding supports path-dependent interpretations of trust development and highlights the importance of historical interactions between citizens and digital institutions.

Fourth, the study introduces a conceptual distinction between digital literacy and digital rights awareness, demonstrating that technological competence alone is insufficient for sustainable trust development. This distinction carries both theoretical and practical significance, suggesting that trust-building efforts must extend beyond technical training to include legal and regulatory awareness. Fifth, the integration of grounded theory and PLS-SEM provides

a methodological contribution by demonstrating an effective approach for developing and validating context-sensitive governance models in emerging digital societies.

Sixth, by positioning the governance-centered framework within the emerging discourse on trust in immersive digital environments, the study contributes to the growing literature on metaverse governance. The framework's emphasis on institutional legitimacy, transparency, and accountability offers a lens for understanding trust dynamics in virtual worlds, where platform governance and algorithmic fairness are critical concerns (Dwivedi et al., 2022; Shin, 2022; Wang et al., 2023).

6.3 Practical and Policy Implications

The findings provide several actionable implications for policymakers, regulators, and digital service providers. At the policy level, governments should prioritize the development of comprehensive digital governance legislation that clearly defines digital rights, institutional responsibilities, privacy protections, and accountability mechanisms. Establishing a coherent legal framework can reduce uncertainty and strengthen public confidence in digital services. At the institutional level, greater coordination among governmental agencies is required to overcome fragmented governance structures. Integrated policymaking and clearly defined responsibilities can improve service consistency and institutional credibility. At the organizational level, public and private digital service providers should treat trust as a strategic asset. Investments in cybersecurity, service quality, transparency, incident response mechanisms, and user-centered design can significantly improve citizens' trust perceptions. At the societal level, digital literacy programs should be expanded beyond technical competencies to include awareness of digital rights, privacy protection, cybersecurity practices, and mechanisms for redress and accountability. Such initiatives can empower citizens and promote more confident participation in digital environments. For immersive digital environments, policymakers should consider how existing governance frameworks can be extended to address platform accountability, virtual asset protection, and algorithmic transparency in metaverse ecosystems. Collectively, these measures can facilitate the transition from technology-centered digital transformation to trust-centered digital governance in both conventional and emerging digital environments.

6.4 Limitations of the Study

Despite its contributions, the study is subject to several limitations. First, the qualitative phase primarily relied on expert perspectives, which may not fully capture the experiences and perceptions of ordinary citizens and end-users. Future studies should incorporate broader stakeholder groups to obtain a more comprehensive understanding of digital trust dynamics. Second, the study was conducted within the specific institutional and regulatory context of Iran. Although some findings may be transferable to other developing countries and to immersive digital environments, further validation is required before generalizing the model across different socio-political and technological contexts.

Third, the quantitative phase employed a cross-sectional design, limiting the ability to examine changes in trust over time. Longitudinal studies are recommended to investigate the evolution of digital trust and the long-term effects of governance reforms. Fourth, the rapid advancement of emerging technologies such as artificial intelligence, digital identity systems, blockchain, and algorithmic governance may alter trust relationships in the future. Additional research is needed to explore how these technologies influence trust formation and governance outcomes. Fifth, while the framework's relevance to immersive environments is conceptually argued, empirical validation in metaverse and virtual platform contexts is needed to confirm its applicability in these settings.

6.5 Future Research Directions

Several avenues for future research emerge from this study. First, future studies may develop and validate a comprehensive Digital Trust Index tailored to developing-country contexts, with potential extensions to capture trust in immersive digital environments. Second, researchers may investigate the relationship between digital trust and social capital using advanced multilevel analytical approaches. Third, machine learning and artificial intelligence techniques could be employed to predict citizens' trust levels based on behavioral and demographic characteristics.

Fourth, data mining and sentiment analysis methods may be used to identify hidden patterns of trust and distrust within digital platforms and social media environments. Fifth, evolutionary game theory may provide valuable insights into the design of regulatory incentives and trust-enhancing governance mechanisms. Sixth, agent-based modeling and reinforcement learning approaches could be employed to simulate interactions among citizens, platforms, regulators, and governmental institutions in complex digital ecosystems, including metaverse and virtual worlds.

Additionally, comparative cross-national studies could investigate how cultural, institutional, and technological factors interact to shape digital trust across different developing and emerging economies. Studies specifically examining trust in immersive environments—including metaverse platforms, virtual reality social spaces, and augmented reality services—could extend the governance-centered framework to these rapidly evolving contexts. Such studies would contribute to a deeper understanding of digital trust dynamics and support the development of more effective governance strategies in the digital age.

Declaration of Competing Interest

The author declares that he has no competing financial interests or known personal relationships that would influence the report presented in this article.

References

- Almarashdah, M. A., Gharaibeh, Z. I. Y., Sial, M. S., & Tahir, M. (2024). The nexus of good e-governance, e-trust, and digital citizenship behaviour: A perspective of emerging economies. *International Journal of Electronic Governance*, 16(4), 468–489.
- Beyene, E., Bedemo, A., & Gebremeskel, A. (2024). Determinants of digital technology development in sub-Saharan African countries: Evidence from panel data analysis. *Energy Informatics*, 7(21), 1–22.
- Duenas-Cid, D. (2024). Trust and distrust in electoral technologies: What can we learn from the failure of electronic voting in the Netherlands (2006/07). *arXiv preprint*.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage.
- Ibor, A., Hooper, M., Maple, C., Crowcroft, J., & Epiphaniou, G. (2025). Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries. *AI & Society*, 40(4), 2729–2750.
- ISACA. (2024). *Digital Trust Ecosystem Framework (DTEF)*. ISACA.
- Jarvenpaa, S. L., & Teigland, R. (2017). Platforms, trust and governance. In *The SAGE Handbook of Information and Communication Technologies* (pp. 123–141). Sage.
- Kitsios, F., & Kamariotou, M. (2023). Digital transformation and trust in virtual environments. *Journal of Business Research*, 156, 113524.
- Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*.
- Luhmann, N. (1979). *Trust and power*. Wiley.

- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- Mazhar, M. U., Khan, A., & Ahmad, S. (2025). Digital trust and public sector transformation: Emerging perspectives in digital governance. *Government Information Quarterly*, 42(1), 101982.
- Mystakidis, S. (2022). Metaverse. *Encyclopedia*, 2(1), 486–497.
- Nosike, C. J. O. (2024). Digitalization in developing countries: Opportunities and challenges. *International Journal of Digital Development Studies*, 8(1), 15–34.
- OECD. (2024). *Building trust in the digital age: OECD digital government outlook 2024*. OECD Publishing.
- Ofosu-Mensah Ababio, J., & Yiadom, E. B. (2024). Digital financial inclusion and inclusive development in lower-middle-income countries: The enabling role of institutional quality. *Journal of Chinese Economic and Foreign Trade Studies*, 17(2–3), 133–151.
- Raheem, S., Addo, A., Shaffakat, S., & Lunberry, D. (2024). Designing for financial inclusion in developing countries: Digital financial service for low-income women in Ghana. *The Information Society*, 40(5), 1–19.
- Rauschnabel, P. A., Felix, R., Hinsch, C., Shahab, H., & Alt, F. (2022). What is XR? Towards a framework for augmented and virtual reality. *Computers in Human Behavior*, 133, 107289.
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Shin, D. (2022). The actualization of meta trust: A critical review of trust in metaverse. *Computers in Human Behavior*, 136, 107378.
- Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.). Sage.
- Tan, T. M., & Salo, J. (2023). Trust in virtual worlds: A review and research agenda. *Journal of Virtual Worlds Research*, 16(1), 1–18.
- United Nations. (2024). *Global Digital Compact: Shared principles for an open, free and secure digital future*. United Nations.
- Van Dijck, J., Poell, T., & De Waal, M. (2023). *The platform society: Public values in a connective world* (Updated ed.). Oxford University Press.
- Vial, G. (2023). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 32(1), 101772.
- Wang, Y., Lee, L. H., Braud, T., & Hui, P. (2023). Digital trust in the metaverse: A systematic literature review. *Telematics and Informatics*, 82, 102009.
- World Economic Forum. (2024). *Digital trust framework and governance principles for the intelligent age*. World Economic Forum.
- Zarifis, A., & Cheng, X. (2023). The six ways to build trust and reduce privacy concern in a central bank digital currency (CBDC). *Electronic Commerce Research and Applications*, 61, 101308.