

Digital Trust as a Strategic Enabler of Innovation in Emerging Technology Ecosystems

¹Sodeeq Ipadeola Olalekan, ¹Boluwatife Gabriel Jesutoye and ²David Chinonso Anih

¹Information Security Department, INHAF Ltd, Greater Manchester, United Kingdom

²Federal University Wukari, Taraba, Nigeria

Corresponding Author: David Chinonso Anih (anah.david@fuwukari.edu.ng)

ABSTRACT

Digital trust has become increasingly important in emerging technology ecosystems, where rapid technological innovation depends on secure, transparent, and reliable digital interactions. Building digital trust can therefore facilitate innovation, collaboration, and sustainable technology adoption. This review examines digital trust as a strategic enabler of innovation in emerging technology ecosystems, with particular attention to governance, identity, security, data, and authenticity. The literature search period spanned 2021 to 2026, and the review was based on peer reviewed journal studies that helped clarify digital trust as a multidimensional condition rather than a vague expression of confidence. Across the literature, digital trust emerges as a practical foundation for adoption, collaboration, ecosystem coordination, and scalable innovation. It is shaped by transparency, explainability, privacy protection, accountability, interoperability, certification, and credible governance signals, alongside technical controls that reduce uncertainty and operational risk. The evidence shows that trust supports innovation by lowering perceived risk, strengthening user acceptance, and making digital systems more usable in real settings. In innovation ecosystems, trust improves collaboration among platform owners, developers, service providers, regulators, and end users, while also supporting retention, satisfaction, and performance. At the governance level, responsible artificial intelligence governance, privacy by design, and cross-border data flow governance appear to function as enabling conditions rather than barriers when they are clear, implementable, and aligned with system design. At the technical level, zero trust architecture, self-sovereign identity, privacy-enhancing technologies, cloud native security, and trustworthy data spaces create layered assurance that protects access, identity, workloads, and data throughout the digital lifecycle. The review also shows that trust is increasingly tied to authenticity, especially in environments shaped by generative artificial intelligence, synthetic media, deepfakes, and provenance concerns. Sectoral evidence indicates that the trust requirements of healthcare, finance, public administration, smart cities, manufacturing, and digital trade differ in emphasis, but share the same underlying logic: Innovation scales more reliably when users and institutions can verify what is happening, who is involved, and whether the system is legitimate. Overall, digital trust should be understood as a structural condition for responsible innovation, not as a secondary feature. Future research should prioritize integrated measurement frameworks, broader inclusion, and more practical models for scaling trustworthy digital infrastructures across sectors and jurisdictions.

KEYWORDS

Digital trust, innovation ecosystems, governance, self sovereign identity, zero trust architecture, data governance, privacy enhancing technologies, authenticity, Artificial Intelligence

Copyright © 2026 Olalekan et al. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.



INTRODUCTION

Digital trust has moved from a soft reputational concern to a strategic asset in emerging technology ecosystems because digital transformation now reshapes organizational design, operating models, and interfirm coordination at the same time. Recent reviews show that digital transformation is not a single technology upgrade, but a broad shift in how firms create value, redraw boundaries, and reorganize routines across internal and external layers^{1,2}. In that setting, innovation depends not only on technical capability, but also on whether users, firms, and regulators believe that the surrounding digital environment is reliable, accountable, and fit for purpose. Trust therefore becomes a governance issue as much as a technology issue, because it influences adoption, experimentation, and the ability to scale new digital solutions across markets^{1,2}.

The trust question becomes even more demanding in the AI era. As artificial intelligence is embedded in credit decisions, health services, mobility systems, and commerce, the literature has increasingly emphasized responsible AI governance as a way of turning ethical principles into operational practice across design, deployment, monitoring, and evaluation³. At the same time, current evidence on trust in AI shows that trust is shaped by both performance and broader concerns such as safety, transparency, accountability, and alignment with human values⁴. This matters because emerging technology ecosystems are now moving faster than traditional oversight structures, and the very speed that makes them innovative can also magnify opacity, bias, error, and misuse. In practical terms, trustworthiness is no longer a decorative feature of digital systems. It is part of what gives them legitimacy, acceptability, and room to grow^{3,4}.

Identity, data, and platform governance sit at the center of this debate. Research on self sovereign identity and digital wallets shows that fragmented identity management, dependence on corporate identity providers, and weak support for verifiable attributes still limit secure and portable digital interaction, while newer identity architectures are designed to improve interoperability and user control⁵. Platform governance is equally important, because digital platforms do not create innovation value automatically. They must be governed in ways that support social options, manage boundary resources, and balance private value with broader social value creation⁶. Data governance adds another layer of urgency. Recent mapping work shows that data governance is a fast-growing but still fragmented field, reflecting persistent challenges around stewardship, quality, control, and coordination even as data-driven innovation accelerates⁷. Taken together, these streams suggest that innovation in emerging technology ecosystems is increasingly limited not by the absence of digital tools, but by the quality of trust relationships surrounding identity, security, data, and authenticity.

This review addresses a clear knowledge gap. Existing studies often examine trust in isolation, within a single technology, sector, or governance layer, while emerging technology ecosystems demand an integrated view that connects governance, identity, security, data, and authenticity across the full innovation stack¹⁻⁷. The aim of this comprehensive review is therefore to synthesize recent evidence on digital trust as a strategic enabler of innovation, clarify the pathways through which it supports adoption and scale, and draw implications for researchers, industry leaders, and policymakers building trustworthy digital infrastructures.

MATERIALS AND METHODS

LITERATURE IDENTIFICATION, SCOPE, AND EVIDENCE SELECTION

The literature considered in this comprehensive review was assembled through a structured and multidisciplinary evidence identification process aimed at capturing the broad and evolving dimensions of digital trust within emerging technology ecosystems. The review drew evidence from major scholarly sources, including Scopus, Web of Science, PubMed/MEDLINE, and Google Scholar, thereby allowing relevant contributions from information systems, cybersecurity, digital governance, health informatics,

technology management, and related fields to be considered within the same analytical framework. The review covered literature published from 2021 to 2026, with emphasis on peer reviewed journal articles, reviews, meta analyses, and empirical studies that contributed directly to the understanding of digital trust, technological innovation, governance, security, identity, data management, and digital authenticity. This broad evidence base was considered appropriate for a comprehensive review because digital trust is inherently multidisciplinary and is rarely examined through a single academic or technological perspective⁸⁻¹⁰.

The identification of relevant literature was guided by several interconnected thematic areas rather than a single set of terms. These areas included digital trust and trustworthiness; innovation, adoption, and technology ecosystems; governance and digital identity; cybersecurity, privacy, and access control; and authenticity, provenance, and verification. Within these themes, related terms such as "digital trust", "trustworthiness", "trust formation", "innovation", "ecosystem", "adoption", "identity", "zero trust", "privacy-enhancing technologies", "data governance", "provenance", and "authenticity" were considered. Additional attention was given to literature addressing artificial intelligence, cloud computing, Internet of Things, blockchain, data spaces, synthetic media, and deepfakes. This approach was important because studies examining trust in emerging technologies do not always explicitly use the term "digital trust". Relevant evidence may instead be presented through concepts such as transparency, credibility, legitimacy, assurance, verification, privacy, or accountability⁸⁻¹⁰.

The scope of the review was therefore deliberately broad enough to accommodate both foundational and applied evidence. Conceptual studies were considered where they helped define the meaning, dimensions, or theoretical basis of digital trust, while empirical and review studies were used to examine how trust operates in practical technology environments. Particular attention was given to evidence describing the relationship between trust and technology adoption, collaboration, governance, security, identity assurance, privacy protection, interoperability, and authenticity. Studies that examined emerging digital environments were especially relevant where they demonstrated how trust can influence the acceptance, use, governance, or scaling of technological innovations. This evidence was examined across different technology domains rather than treating digital trust as an isolated property of a particular system or platform⁸⁻¹⁰.

To preserve the scholarly focus of the review, peer-reviewed journal literature formed the principal evidence base. Grey literature, policy documents, standards, and vendor materials were considered only as contextual sources where necessary for interpretation and were not relied upon as the main scholarly evidence. This distinction helped maintain consistency in the quality of the material used while acknowledging that digital trust is also shaped by regulatory, institutional, and industry environments. The evidence was subsequently organized around the major dimensions identified across the literature, including governance, identity, security, data, transparency, privacy, and authenticity. This organization enabled the review to move beyond a simple description of individual technologies and instead examine the broader relationships through which digital trust supports innovation, collaboration, legitimacy, and sustainable participation in emerging technology ecosystems⁸⁻¹⁰.

Overall, the evidence identification and selection process was designed to provide a comprehensive view of digital trust as a multidimensional and evolving phenomenon. By bringing together literature from complementary research traditions, the review was able to consider both the technical mechanisms that create assurance and the institutional, organizational, and human factors that determine whether such assurance is accepted and sustained. The resulting body of evidence provided the basis for synthesizing digital trust across its major dimensions and for examining its role as an enabling condition for responsible innovation in emerging technology ecosystems⁸⁻¹⁰.

Digital trust: Conceptual foundations and core dimensions: Recent literature converges on the view that digital trust is not a single feeling of confidence, but a layered judgment about whether people, processes, and technologies can be relied on in a secure digital environment. A recent systematic survey defines digital trust as confidence in people, processes, and technology that sustain a secure digital environment, while also showing that openness sits alongside ability, benevolence, integrity, privacy, and data protection as a meaningful part of the construct¹¹. That is a useful shift, because it moves the concept away from a narrow cybersecurity reading and toward a broader socio-technical one in which trust depends on the quality of the entire digital environment, not just on whether a system has been hardened against attack.

The trust literature on digital platforms adds another layer to this definition. A meta-analysis of 74 primary studies found that trusting beliefs, attitude, platform provider image and reputation, structural assurance, perceived usefulness, and perceived enjoyment all have positive effects on trusting intention in digital platforms¹². In practical terms, this means that digital trust is shaped both by objective assurance mechanisms and by user perception. People trust platforms more readily when they can see credible signals of competence, reliability, and consistency, but also when the platform feels useful, understandable, and socially legitimate. That combination of technical assurance and perceived value is exactly why digital trust has become central to emerging technology ecosystems rather than peripheral to them¹².

Transparency is one of the most important operational dimensions of digital trust, especially in systems where the logic of decision-making is difficult to inspect. A user-based study in intelligent systems found that transparency plays an important indirect role in acceptance by regulating trust and perceived performance, even when it does not act as a simple direct cause of adoption¹³. This is highly relevant for emerging technologies such as AI, recommendation engines, and automated agents, where black box behavior can undermine confidence even when performance is technically strong. The literature therefore points to a broader set of trust dimensions that now includes cybersecurity, safety, interoperability, privacy, transparency, redressability, ethics, fairness, and sustainability, because users and institutions increasingly evaluate systems across the whole lifecycle of use rather than at the point of first adoption¹¹⁻¹³.

Table 1 brings together the main definitions of digital trust and the core dimensions highlighted across the key sources. It helps show how the concept moves from a narrow security idea to a broader trust-based view of digital environments.

Digital trust as a strategic enabler of innovation: Digital trust is strategically valuable because it lowers the friction that normally slows adoption, collaboration, and scaling. In innovative small and medium-sized firms, digital technology adoption is strongly shaped by adoption costs, top management support, human resources, digital culture, and trading partner pressure, with digital culture emerging as a particularly influential predictor¹⁴. That finding matters for innovation ecosystems because trust is what allows digital culture to become productive instead of merely aspirational. When firms trust their partners, their systems, and the governance environment, they are more willing to invest in new tools, to learn from them, and to coordinate across organizational boundaries. Trust therefore does not merely accompany innovation; it helps create the conditions under which adoption becomes realistic and durable¹⁴.

The trust-based view of innovation ecosystems shows that trust works through network collaboration, interdependency, value co-creation, and shared innovation objectives¹⁵. The important insight is that no single trust dimension is sufficient by itself. Ability, benevolence, and integrity need to function together if ecosystem actors are to exchange knowledge, share risk, and coordinate complementary capabilities.

Table 1: Definitions and dimensions of digital trust across major sources

Working definition	Core dimensions emphasized	Citation(s)
Confidence in people, processes, and technology in a secure digital environment	Ability, benevolence, integrity, openness, privacy, data protection	Wanner <i>et al.</i> ¹¹
Trusting intention in digital platforms as an outcome of multiple belief and assurance signals	Trusting beliefs, reputation, structural assurance, usefulness, enjoyment	Steinbruch <i>et al.</i> ¹²
Trust in intelligent systems is shaped by how transparent and acceptable the system appears to end users	Transparency, perceived performance, acceptance, explanation quality	Fernández-Portillo <i>et al.</i> ¹³

This table compares major working definitions of digital trust with the dimensions most often emphasized in the literature. It highlights ability, benevolence, integrity, openness, privacy, trust beliefs, reputation, structural assurance, usefulness, enjoyment, transparency, perceived performance, acceptance, and explanation quality

Table 2: Mechanisms linking digital trust to innovation outcomes

Mechanism	How trust operates	Innovation outcome	Citation(s)
Adoption support	Reduces perceived risk and organizational hesitation	Faster uptake of new digital tools	Faiz <i>et al.</i> ¹⁴
Collaboration and co-creation	Encourages knowledge sharing and shared problem solving	Stronger ecosystem coordination	Tsai <i>et al.</i> ¹⁵
Retention and performance	Keeps stakeholders engaged and satisfied	Better business performance and renewal	Liu <i>et al.</i> ¹⁶

This table shows the practical mechanisms through which digital trust improves innovation outcomes. It links adoption support, collaboration and co-creation, and retention and performance to faster uptake, stronger coordination, and better renewal

This is especially relevant in emerging technology ecosystems where value is rarely produced by one firm alone. Instead, innovation depends on a chain of trusted relationships among platform owners, developers, service providers, regulators, and end users. Without that trust, collaboration becomes defensive, knowledge sharing becomes partial, and ecosystem growth slows down¹⁵.

The same pattern appears in digital business ecosystem research. A large-scale study of Spanish SMEs found that digital business ecosystems are positively associated with customer and employee satisfaction, and that employee satisfaction in particular improves business performance¹⁶. That is an important reminder that trust is not only about preventing harm. It is also about enabling positive organizational outcomes such as user retention, service quality, internal commitment, and willingness to continue participating in a digital environment. When stakeholders feel that digital systems are dependable and well governed, they stay engaged longer, collaborate more freely, and are more likely to support experimentation. In that sense, digital trust is one of the hidden infrastructure layers of innovation capability because it connects adoption, satisfaction, and performance into a single upward cycle¹⁴⁻¹⁶.

Table 2 explains the main ways digital trust supports innovation outcomes. It connects trust to faster adoption, stronger collaboration, and better retention and performance.

Governance, security, identity, and data foundations of trust: A credible digital trust environment depends on governance that is strict enough to reduce abuse and flexible enough to support legitimate use. Zero trust architecture is central here because it rejects inherited trust and instead requires precise authentication, minimal authorization, and continuous verification for every access request¹⁷. Recent zero trust literature shows that this model is no longer an abstract security slogan. It is now treated as a practical implementation strategy for organizations that need to protect resources in remote, hybrid, and distributed environments. The architecture is particularly relevant to innovation ecosystems because it allows firms to collaborate without assuming that internal network location alone is a reliable trust signal^{17,18}.

A broader survey of zero trust research in IoT confirms that the field has matured from a concept to an implementation-oriented security paradigm, especially where device heterogeneity, remote connectivity, and continuous threat exposure make conventional perimeter defense weak¹⁸. For emerging technology

Table 3: Governance and technical controls for building digital trust

Control layer	Main function	Why it matters for trust	Citation(s)
Zero trust architecture	Continuous verification and least privilege access	Prevents inherited trust and limits lateral risk	Glöckler <i>et al.</i> ¹⁷ Ramamoorthi <i>et al.</i> ¹⁸
Identity assurance and SSI	Cryptographic identity and wallet based attestations	Supports usable and privacy aware assurance	Liang <i>et al.</i> ¹⁹ Feretzakis <i>et al.</i> ²⁰
Trustworthy data spaces	Governance, traceability, and standardization	Enables lawful sharing and cross border compliance	Polcumpally <i>et al.</i> ²¹

This table presents the main controls that make digital trust operational in real systems. Zero trust means continuous verification, SSI means self sovereign identity, and the table also covers trustworthy data spaces as a route to lawful sharing and cross border compliance

ecosystems, the importance of this shift is straightforward: trust must be earned continuously, not granted once and forgotten. This is why identity assurance, context-aware access control, and continuous monitoring are becoming non-negotiable design features in cloud, IoT, and platform-based systems. The security literature increasingly treats these features not as separate tools but as mutually reinforcing controls that support verifiable trust at scale^{17,18}.

Identity is the bridge between security and trust. A systematic review of enterprise identity and access management found that cyberattacks and data breaches frequently originate in weak IAM systems, and that self sovereign identity can improve manageability, usability, and least privilege enforcement through cryptographic attestations stored in digital wallet applications¹⁹. A complementary rapid review of federated digital identifiers found that these systems can support patient accessible electronic health records through single sign on, but adoption remains uneven and appears to improve where opt out registration and easier user onboarding are present²⁰. Taken together, the message is clear: Identity systems do not build trust simply because they are digital. They build trust when they are usable, portable, privacy aware, and able to reduce administrative friction while still preserving assurance^{19,20}.

Data governance closes the loop by defining how data may flow across organizational and national boundaries without losing legitimacy. A 2025 review of trustworthy data spaces proposes a blockchain based collaborative trust mechanism and a technology governance standardization framework that seeks to make data available without making it visible, while still preserving auditability and cross border compliance²¹. That is exactly the kind of logic needed in modern ecosystems, where cross border data flows, privacy, interoperability, and traceability must coexist. Trust is therefore not only about protection from bad actors. It is also about the ability to demonstrate compliance, preserve provenance, and support lawful sharing across complex institutional boundaries¹⁹⁻²¹.

Table 3 outlines the key governance and technical controls that build digital trust. It shows how zero trust, identity assurance, and trustworthy data spaces work together to reduce risk and support lawful use.

Emerging technology ecosystems and the review synthesis model: Emerging technology ecosystems expand the meaning of trust beyond classic security concerns. In generative AI and large language models, a recent narrative review shows that privacy preserving techniques such as differential privacy, federated learning, homomorphic encryption, secure multiparty computation, and post quantum cryptography are increasingly important because model training itself can expose sensitive data or enable inference attacks²². This matters because AI systems are often embedded in broader innovation ecosystems where trust is judged not only by whether the system is accurate, but also by whether it respects privacy, resists leakage, and can be deployed responsibly at scale. In other words, trust is becoming a design requirement for AI infrastructure, not just an ethical aspiration²².

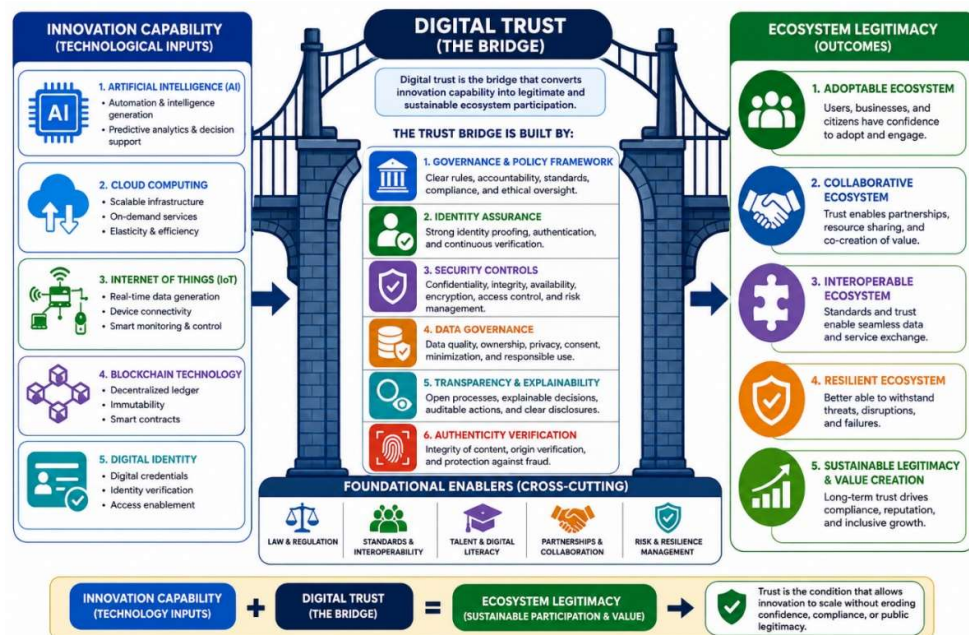


Fig. 1: Conceptual model of digital trust as the bridge between innovation capability and ecosystem legitimacy¹¹⁻²⁴

The figure 1 shows the relationship between innovation inputs, digital trust, and ecosystem legitimacy, with digital trust positioned as the central bridge that supports legitimate and sustainable ecosystem participation. Abbreviations: AI, artificial intelligence; IoT, Internet of Things; digital trust, confidence in the integrity, security, transparency, and authenticity of digital systems

Table 4: Emerging technology ecosystem matrix and trust implications

Ecosystem	Main trust issue	Trust implication	Citation(s)
AI and LLMs	Privacy leakage, model inversion, inference attacks	Privacy preserving design is part of trust	Lao <i>et al.</i> ²²
Blockchain and data spaces	Governance, auditability, standardization	Trust requires verifiable coordination	Polcumpally <i>et al.</i> ²¹
Multimedia authenticity	Deepfakes, synthetic media, provenance	Trust now includes authenticity assurance	Glassberg <i>et al.</i> ²⁴

This table compares trust issues across AI and LLMs, blockchain and data spaces, and multimedia authenticity. AI means artificial intelligence, LLMs means large language models, and the table shows that privacy preserving design, verifiable coordination, and authenticity assurance are all part of digital trust

Blockchain research reinforces that point by showing that governance and trust are now treated as multi sector issues involving accountability, standardization, and verification rather than only decentralization²³. A recent thematic systematic review found that blockchain governance needs to be read through trust, institutional design, and sector specific coordination, not just through technical consensus mechanisms²³. When applied to digital identity, data spaces, or multimedia provenance, blockchain can support auditable records and tamper resistance, but it does not create trust automatically. Trust still depends on governance design, usable verification, and the credibility of the surrounding institutions. That is why the strongest applications of blockchain in current literature are those that combine technical traceability with practical policy and compliance structures²¹⁻²³.

Authenticity has become the newest frontier of digital trust because synthetic media now threatens the credibility of visual and audiovisual evidence itself. A 2025 study on AI and authenticity found that young people verify deepfake videos by checking image, sound, narrative, and intuition, while also assessing the possible consequences and social context of the content²⁴. This is important because it shows that authenticity checks are moving from backend technical problems into everyday user judgment. The implication for digital trust is direct: future ecosystems must provide provenance, labeling, and verification tools that help users decide what is real, what is synthesized, and what has been manipulated. Trust now extends beyond data security into the authenticity of what people see, hear, and share²²⁻²⁴.

Table 4 compares major emerging technology ecosystems and the trust issues each one raises. It shows how privacy, auditability, governance, and authenticity shape trust across AI, blockchain, and multimedia content.

Figure 1 presents the conceptual model showing digital trust as the bridge that converts innovation capability into ecosystem legitimacy, as discussed in subsection 2.5. It illustrates how AI, cloud computing, IoT, blockchain technology, and digital identity are enabled by governance, identity assurance, security, data governance, transparency, and authenticity verification to produce adoption, collaboration, interoperability, resilience, and sustainable value.

RESULTS AND DISCUSSION

DIGITAL TRUST DIMENSIONS MOST ASSOCIATED WITH INNOVATION PERFORMANCE

Across the recent literature, the digital trust dimensions most consistently associated with innovation performance are transparency, explainability, privacy protection, perceived accuracy, nonmaliciousness, and the presence of recognizable governance signals such as certification, standards, and accountable oversight. A useful way to read the evidence is that trust does not act as a single vague sentiment; it works as a bundle of practical assurances that lowers uncertainty, reduces the perceived cost of experimentation, and makes adoption feel safe enough to scale. In the 2024 review of trust in AI, trustworthiness is treated as a multi layer construct that includes both technical and axiological dimensions, with factors such as transparency, explainability, certification, standards, and data governance repeatedly appearing as trust building conditions for human machine interactions²³. That finding matters because innovation performance in digital ecosystems rarely depends only on technical novelty. It depends on whether users, firms, and institutions believe the system is legible, governable, and sufficiently bounded to be used in high value settings²³.

Transparency and explainability stand out because they convert black box behavior into inspectable behavior. The 2025 study on AI powered digital agents shows that design and transparency are not decorative features; they shape whether people feel able to rely on an agent, delegate tasks to it, and keep using it in realistic workflows²⁴. This is important for innovation because the early phase of adoption is often fragile. Users may test a new tool once, but they scale it only when the system's logic, error profile, and interface behavior remain understandable enough for them to manage risk. In that sense, transparency does not simply improve trust after the fact. It improves the conditions under which innovation can move from pilot use to routine use, which is a major distinction in digital transformation²⁴.

A second recurring trust dimension is the perceived quality and safety of the output itself. The 2025 comparative study of generative AI tools among students, teachers, and researchers found that trust was closely tied to accuracy, relevance, privacy protection, and nonmaliciousness²⁵. This is a particularly revealing combination because it shows that users are not only evaluating whether an output is technically correct. They are also evaluating whether the tool respects privacy, avoids harmful behavior, and produces results that are fit for the task at hand²⁵. For innovation performance, that means the trust question is domain sensitive. A tool can be exciting and still fail to scale if it produces weak, unsafe, or inappropriate results in settings where users cannot tolerate those failures. The more high stakes the use case, the more the innovation depends on trust qualities that are visible in everyday use, not merely in marketing claims²⁵.

Taken together, the literature suggests that the innovation value of digital trust comes from a cumulative effect. Transparency helps users understand the system. Accuracy and relevance help them depend on the output. Privacy protection helps them share data. Nonmaliciousness helps them believe the system will not turn against their interests. Governance signals help them believe the innovation is not an unaccountable experiment. When these elements are aligned, adoption tends to be more durable, scaling is less brittle, and user confidence is more likely to survive the first operational failure or surprise interaction²³⁻²⁵.

Table 5: Summary of evidence by digital trust dimension

Digital trust dimension	What the evidence shows	Innovation implication	Citation(s)
Technical trustworthiness and governance signals	Trust is shaped by standards, certification, explainability, and data governance, not only by performance claims	Better legitimacy, lower uncertainty, easier institutional adoption.	Azarov and Tulupyeva ²³
Transparency and explainability	Users trust AI powered agents more when behavior is legible and design supports inspection	Faster movement from pilot testing to routine operational use.	Glassberg <i>et al.</i> ²⁴
Accuracy, relevance, privacy, and nonmaliciousness	Trust in generative AI depends on output quality, task fit, and protection against harmful use	Stronger user confidence and more sustainable adoption in real workflows	Đerić <i>et al.</i> ²⁵

This table summarizes the evidence linking specific trust dimensions to innovation performance. AI here refers to artificial intelligence, while the table highlights standards, certification, explainability, data governance, transparency, relevance, privacy, and nonmaliciousness as practical trust signals

Table 5 summarizes the digital trust dimensions most strongly associated with innovation performance. It highlights technical trustworthiness, transparency, explainability, and output quality as the main drivers of durable adoption.

Governance and regulatory enablers of trust based innovation: The strongest governance finding in the recent literature is that regulation need not function as an innovation brake. In the best cases, it acts as a coordination layer that makes experimentation safer, transactions more predictable, and responsibilities easier to assign. The 2024 review on responsible artificial intelligence governance argues that AI governance has to be understood through structural, relational, and procedural practices, meaning that institutions, communication patterns, and operational routines all matter together²⁶. This is a useful shift because it moves governance beyond the narrow idea of compliance paperwork. In practice, innovation ecosystems need policy clarity about who is accountable, how risk is assessed, how disputes are handled, and what internal controls must exist before a system is deployed widely²⁶. Where those conditions are visible, regulation can reduce transaction costs rather than increase them.

Privacy regulation also becomes an innovation enabler when it is embedded into system design rather than added as an afterthought. The 2024 study on national identification systems shows that privacy by design is strongest when stakeholders understand the model, implementation guidance is available, and privacy controls are built into the architecture of the system itself²⁷. That lesson travels far beyond identity systems. It suggests that regulatory legitimacy depends on practical implementability. If the rules are too abstract, poorly communicated, or technically detached from system design, trust becomes uneven and innovation slows because organisations do not know how to comply confidently²⁷. By contrast, rights based policy is strongest when it gives developers and institutions a usable framework for building systems that protect individuals without collapsing data utility.

Cross border data governance is now another central enabling condition. The 2026 analysis of Latin American and African perspectives on cross border data flows shows that policy debates are increasingly focused on trusted data use, digital trade, privacy rights, interoperability, and the tension between regulatory sovereignty and open data mobility²⁸. This is important because emerging technology ecosystems often depend on data that travels across borders, cloud regions, vendors, and legal jurisdictions. If those flows are blocked or made unpredictable, innovation becomes locally trapped and globally fragmented. The paper indicates that policy directions in organizations such as the OECD and the European Union continue to emphasize trustworthy data use and legal pathways for cross border transfer, rather than unrestricted circulation or complete data localization²⁸. The deeper point is that innovation thrives when policy makes lawful data movement more dependable, not when it simply announces abstract openness.

Table 6: Policy instruments and governance models supporting trusted innovation

Policy or governance instrument	Core function	Why it supports innovation	Citation(s)
Responsible AI governance	Aligns structural, relational, and procedural practices around accountability and risk control	Clarifies responsibility and lowers institutional uncertainty	Fikardos <i>et al.</i> ²⁶
Privacy by design in identity systems	Embeds privacy into system architecture and implementation	Makes privacy protection operational rather than symbolic	Abomhara <i>et al.</i> ²⁷
Cross border data flow governance	Supports trusted transfer, interoperability, and rights protection across jurisdictions	Enables international scale without destroying legal confidence	Callo-Müller and Sucker ²⁸

This table focuses on policy tools that make innovation more trustworthy in practice. AI means artificial intelligence, and the table shows how accountability, privacy by design, and cross border data flow governance lower uncertainty and support scale

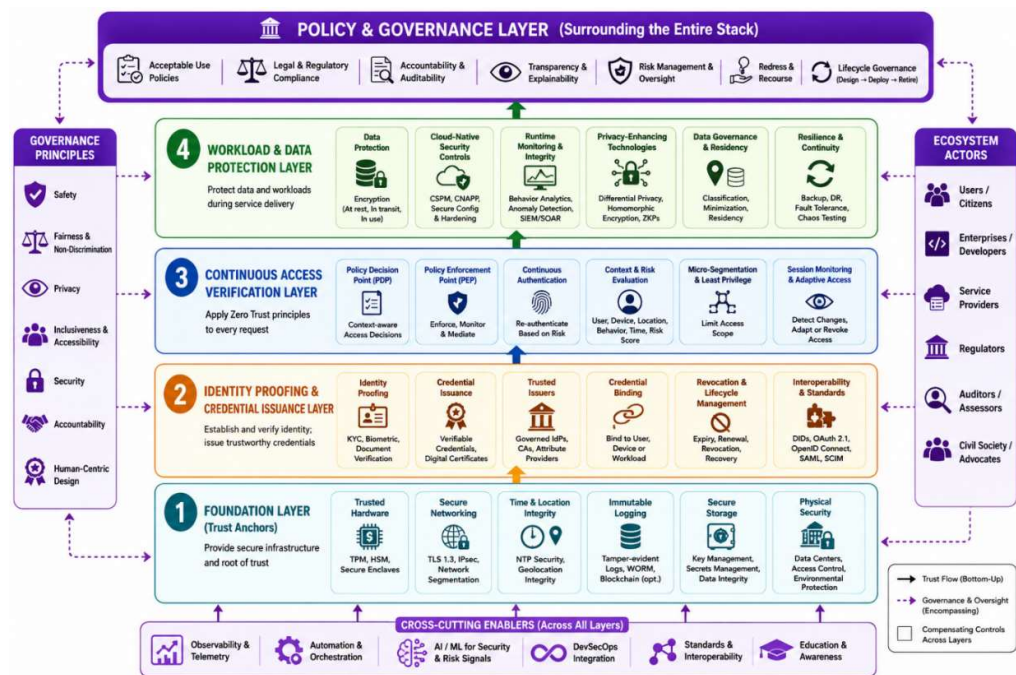
The common thread across these governance and regulatory studies is that trust based innovation depends on policy precision. Governance is not most effective when it is maximal or minimal. It is most effective when it creates clear operating boundaries, transparent accountability structures, and durable rights protections that allow data, models, and services to move with fewer surprises. That is why governance is increasingly being treated as an innovation infrastructure in its own right: it provides the legal and institutional confidence needed for adoption, scaling, and cross border collaboration²⁶⁻²⁸.

Table 6 presents the policy instruments and governance models that support trusted innovation. It shows how responsible AI governance, privacy by design, and cross border data flow governance make innovation safer and more scalable.

Technical enablers: Zero trust, digital identity, PETs, and authenticity: At the technical layer, the literature shows a decisive shift away from perimeter based trust and toward continuous verification. The 2024 systematic review on Zero Trust VPN argues that secure access in hybrid and remote work environments should be governed by identity, device compliance, context awareness, and least privilege rather than by the assumption that a user or network segment is trustworthy by default²⁹. That is a major conceptual change for emerging technology ecosystems. It means trust is not granted once and for all at login. It is continuously evaluated against changing conditions such as device health, access patterns, and session behavior²⁹. For innovation, this matters because the more distributed an ecosystem becomes, the more dangerous traditional perimeter security becomes. Zero trust reduces the blast radius of compromise and makes collaboration safer across organisational boundaries.

Identity is the second pillar of this technical trust stack. The 2025 analysis of self sovereign identity and digital wallets shows that current identity systems remain fragmented, prone to lock in, and often weak at presenting machine verifiable attributes in a reusable way³⁰. Digital wallets and self sovereign identity models respond to that problem by enabling users and organisations to present trusted claims without exposing more data than necessary³⁰. That is highly relevant for innovation because identity reuse is one of the hidden bottlenecks in digital ecosystems. When every service rebuilds identity from scratch, friction rises, onboarding slows, and trust becomes expensive. When credentials become portable and verifiable, trust becomes reusable and innovation can spread across platforms with less administrative overhead³⁰.

The third technical layer is cloud native security and privacy enhancing tooling. The 2025 survey of privacy enhancing and trust centric cloud native security techniques describes a practical stack that includes encryption, identity and access management, service mesh controls, runtime protection, endpoint security, container image scanning, and security monitoring³¹. The value of this work is that it shows trust is not only a user interface question or a policy question. It is also a deployment question. Systems need controls at build time, deployment time, and runtime if they are going to sustain trust under actual operational pressure³¹. In complex digital ecosystems, the promise of innovation is often undermined by mundane security gaps. Cloud native controls close those gaps by reducing attack surfaces and preserving the integrity of data and workloads while services are being scaled.

Fig. 2: Layered trust architecture for emerging technology ecosystems²⁹⁻³¹

The diagram shows four interconnected layers: Foundation Layer, Identity Proofing and Credential Issuance Layer, Continuous Access Verification Layer, and Workload and Data Protection Layer, all enclosed by Policy and Governance. Abbreviations: KYC: Know your customer, TPM: Trusted platform module, HSM: Hardware security module, TLS: Transport layer security, IPsec: Internet protocol security, NTP: Network time protocol, WORM: Write once read many, CA: Certificate authority, IdP: Identity provider, PDP: Policy decision point, PEP: Policy enforcement point, CSPM: Cloud security posture management, CNAPP: Cloud native application protection platform, SIEM: Security information and event management, SOAR: Security orchestration, automation and response, ZKP: Zero knowledge proof, DID: Decentralized identifier, OAuth: Open authorization, OpenID Connect, OpenID connect protocol, SAML: Security assertion markup language, SCIM, System for cross domain identity management, AI/ML: Artificial intelligence/Machine learning and DevSecOps: Development, security, and operations

Table 7: Technical trust mechanisms and representative use cases

Technical mechanism	Main risk reduced	Representative use case	Citation(s)
Zero trust access control	Lateral movement, over privileged access, and insecure remote access	Hybrid and remote work environments	Zohaib <i>et al.</i> ²⁹
Self sovereign identity and digital wallets	Identity fragmentation, lock in, and unnecessary data exposure	Cross platform credential presentation and reusable verification	Schuetz <i>et al.</i> ³⁰
Cloud native security and PET oriented controls	Runtime compromise, data leakage, and weak workload assurance	Containerised services, distributed applications, and platform security	Arif <i>et al.</i> ³¹

This table lays out the technical building blocks of trust in distributed digital environments. PETs means privacy enhancing technologies, and the table pairs zero trust access control, self sovereign identity, and cloud native security with their main risks and use cases

Taken together, zero trust, portable identity, and cloud native security create a layered architecture of assurance. Zero trust governs access. Identity systems establish who or what is interacting. Cloud security tooling protects the workload, the data, and the service environment after access is granted. The practical implication is that trust cannot be outsourced to a single gatekeeper. It has to be engineered across multiple technical layers so that compromise in one layer does not collapse the entire ecosystem. In this sense, technical trust is not a static certification state. It is an operational discipline that must be maintained continuously²⁹⁻³¹.

Table 7 presents the main technical trust mechanisms and their representative use cases. It connects zero trust access control, self sovereign identity, and cloud native security to the practical needs of distributed digital systems.

Figure 2 supports Subsection 3.3 by presenting a layered trust architecture for emerging technology ecosystems, moving from foundation controls and identity assurance to continuous access verification, workload and data protection, and overarching policy governance.

It shows how trust is cumulative, with each layer compensating for weaknesses in the others to create a resilient, zero trust aligned ecosystem.

Sectoral applications of digital trust in emerging technologies: Sectoral evidence shows that digital trust matters most when the stakes are high and the consequences of failure are visible. In healthcare and finance, trust is tied to the handling of sensitive information, regulatory compliance, and the ability to process data without exposing it unnecessarily. The 2024 survey of confidential computing makes this point clearly by showing that secure computation environments are increasingly important for data protection and privacy preserving processing, especially where organisations need to work on sensitive data without revealing raw inputs³². That logic is directly relevant to healthcare analytics, financial services, and other regulated environments where data utility is valuable but disclosure risk is unacceptable. In these settings, innovation is not just about speed or scale. It is about whether institutions can safely use data that would otherwise remain locked in silos³².

Public administration and smart city systems show another side of the same problem. The systematic literature review on digital technologies in public administration networks finds that AI, blockchain, big data, and social media are being used to support public services, emergency response, public safety, healthcare, and education, while trust remains a relational dimension shaped by transparency, communication, and agility³³. That is a crucial result because it reminds us that public sector innovation is not simply technical modernisation. It is a social contract problem. Citizens must believe that the systems handling their data are understandable, fair, and accountable. When that belief exists, digital public services can spread more quickly and integrate across agencies more effectively³³. Smart city projects depend on this same logic, because sensors, platforms, and data sharing arrangements will not deliver their full value unless cities can convince residents that the underlying systems are legitimate and well governed.

Manufacturing and digital trade offer a different but related case. The 2025 literature review on blockchain in manufacturing management and industrial engineering concludes that blockchain can improve transparency, decision making, operational efficiency, trust, traceability, smart contracts, sustainability, and compliance, while also improving interoperability across supply chains³⁴. This matters because modern manufacturing is increasingly distributed, with production, logistics, certification, and supplier coordination spread across multiple organisations and jurisdictions. Digital trust therefore becomes an enabling condition for industrial coordination. A manufacturer can only rely on a digital supply chain if provenance, records, and transaction logic are sufficiently credible to support procurement, quality control, and cross border exchange³⁴. The same logic extends to digital trade, where trusted records and interoperable verification reduce frictions in documentation, payment, and compliance.

The cross sector picture is therefore not one of identical trust needs, but of differentiated trust functions. Healthcare and finance depend heavily on confidentiality and controlled computation. Public administration and smart cities depend on legitimacy, transparency, and interagency coordination. Manufacturing and digital trade depend on traceability, verification, and interoperable records. The common denominator is that trust reduces friction and makes innovation adoptable, but the trust instrument changes by sector. In some sectors, the most important question is who can see the data. In others, it is whether records can be verified end to end. In still others, it is whether citizens or users can believe that systems are fair and accountable enough to use repeatedly³²⁻³⁴.

Table 8: Sector-by-sector effects of digital trust on innovation and adoption

Sector	Dominant trust need	Innovation or adoption effect	Citation(s)
Healthcare and finance	Confidential processing, privacy preservation, and secure computation	Enables analytics and service delivery without exposing sensitive inputs	Feng <i>et al.</i> ³²
Public administration and smart cities	Transparency, communication, and relational legitimacy	Strengthens citizen uptake and interagency coordination	Sienkiewicz-Małyjurek and Zyzak ³³
Manufacturing and digital trade	Traceability, verification, and interoperable records	Supports supply chain reliability, compliance, and cross border exchange	Hariyani <i>et al.</i> ³⁴

This table compares how digital trust works across different sectors and why the trust need changes by context. It shows that confidentiality, transparency, legitimacy, traceability, and verification matter differently in healthcare, public administration, manufacturing, and digital trade

Table 8 shows how digital trust affects innovation and adoption across sectors. It compares healthcare and finance, public administration and smart cities, and manufacturing and digital trade.

CHALLENGES, GAPS, AND FUTURE RESEARCH DIRECTIONS

Despite the progress reflected in the literature, several unresolved issues continue to shape the digital trust agenda. First, privacy enhancing technologies are promising, but their adoption remains uneven because technical utility, governance alignment, and implementation cost do not always move together. The 2024 review of privacy enhancing technologies in biomedical data science shows that these tools can broaden the use of sensitive data by allowing analysis without full exposure, yet the review also makes clear that privacy preserving approaches still face practical hurdles in deployment, interoperability, and responsible scaling³⁵. The broader lesson is that technical capability does not automatically translate into organisational uptake. Future research needs to examine what kinds of incentives, standards, and operating models make PETs routine rather than exceptional³⁵.

Second, deepfake and synthetic media risks are now a major trust problem across digital ecosystems. The 2024 human rights analysis of generative AI and deepfakes highlights the dangers of manipulation, blackmail, abusive content, and misinformation, all of which can erode confidence in digital communication and undermine democratic and social institutions³⁶. The important research gap here is that detection alone is not enough. Systems increasingly need provenance, watermarking, verification, and accountability mechanisms that prevent authenticity failure earlier in the content lifecycle³⁶. This matters for innovation because a platform that cannot reliably distinguish genuine from synthetic content will face rising verification costs, reputational risk, and user scepticism. Trust research therefore needs to move beyond access and privacy to include the integrity of the content itself³⁶.

Third, cross-border asymmetry remains a persistent governance problem. The 2026 study of Latin American and African approaches to cross-border data flows shows that fragmentation, regulatory sovereignty, interoperability, and digital trade are now tightly linked in global policy debates³⁷. The implication is that digital trust is not evenly distributed across jurisdictions. Larger economies may have more regulatory capacity, stronger legal infrastructures, and more influence over platform standards, while smaller or lower-capacity jurisdictions may bear higher compliance burdens relative to their market power³⁷. Future work should therefore examine how trust based innovation can be made more inclusive across borders, especially for firms and public institutions that must operate with constrained legal and technical resources.

A fourth and broader gap concerns measurement. The literature repeatedly shows that trust is multidimensional, but the field still lacks a stable way to measure digital trust across sectors, regions, and technology types. Some studies emphasize perceived transparency and explainability³⁵⁻³⁷. Others emphasize privacy, nonmaliciousness, and output relevance³⁵⁻³⁷. Governance studies focus on accountability and procedural legitimacy³⁵⁻³⁷. Security studies focus on access control, identity, and runtime

Table 9: Research gaps, limitations, and future agenda for digital trust studies

Research gap	What current studies show	Future research priority	Citation(s)
PET adoption and implementation	PETs are promising but difficult to scale in real settings	Study incentives, interoperability, and operational models for routine use	Cho <i>et al.</i> ³⁵
Deepfake and misinformation governance	Synthetic media can undermine authenticity and social trust	Develop provenance, watermarking, verification, and accountability systems	Moreno ³⁶
Cross border trust asymmetry	Data flow governance differs across regions and creates uneven burdens	Design more inclusive, interoperable, and capacity aware governance models	Klingbeil <i>et al.</i> ³⁷

This table brings together the main research gaps and future priorities in the field. PETs means privacy enhancing technologies, and the table points to the need for better incentives, provenance tools, accountability systems, and more inclusive cross border governance

assurance³⁵⁻³⁷. Future research should therefore move toward integrated measurement frameworks that capture not only whether users say they trust a system, but also whether that trust is justified, durable, and transferable across contexts. That is especially important in emerging technology ecosystems, where trust can easily be overstated in early adoption phases and then quickly collapse when the first meaningful failure occurs³⁵⁻³⁷. The most promising future agenda is therefore interdisciplinary. It should connect governance research, security engineering, human centered design, and sector specific adoption studies. It should also examine inclusion, because trust is not experienced equally by all users. Some groups face greater exposure to surveillance, discrimination, or exclusion, and therefore need stronger assurances before they can benefit from digital innovation. Across the reviewed literature, the message is consistent: digital trust is not a soft supplement to innovation. It is a structural condition for innovation that wants to scale responsibly across borders, sectors, and social groups³⁵⁻³⁷.

Table 9 outlines the major research gaps, limitations, and future directions in digital trust studies. It focuses on PET adoption, deepfake governance, and cross border trust asymmetry as the main unresolved areas.

CONCLUSION

Digital trust has emerged from being a background concern to becoming a structural condition for innovation in emerging technology ecosystems, because adoption, collaboration, and scale now depend on confidence in governance, identity, security, data, and authenticity.

The review shows that trust is best understood as a layered and measurable condition, shaped by transparency, explainability, privacy protection, accountability, interoperability, and credible oversight rather than by technical performance alone. At the governance level, responsible AI governance, privacy by design, and cross border data flow governance stand out as practical enablers that can support innovation when they are clear, usable, and aligned with system design. At the technical level, zero trust architecture, self sovereign identity, privacy enhancing technologies, cloud native security, and trustworthy data spaces provide the continuous assurance needed for distributed digital environments to function safely. The evidence also confirms that digital trust is not uniform across sectors, since healthcare, finance, public administration, smart cities, manufacturing, and digital trade each require different trust mechanisms to support adoption and legitimacy. Authenticity has become an especially urgent concern, as generative AI and deepfakes have expanded the need for provenance, verification, watermarking, and accountability across digital communication systems. Taken together, the findings suggest that digital trust is not a soft complement to innovation, but the hidden infrastructure that makes innovation durable, governable, and socially acceptable. Future research should develop integrated measurement frameworks that capture whether trust is justified, durable, transferable, and comparable across sectors, regions, and technology types. Further studies should also examine how to make privacy enhancing technologies easier to deploy, how to strengthen provenance based defenses against synthetic media, and how to reduce cross border trust asymmetry through more inclusive governance models. Overall, advancing trustworthy innovation will require interdisciplinary work that links governance research, security engineering, human centered design, and sector specific adoption studies so that digital ecosystems can scale with confidence and accountability.

SIGNIFICANCE STATEMENT

Digital trust is identified in this manuscript as a foundational condition for innovation in emerging technology ecosystems, integrating governance, identity, security, data, and authenticity into a coherent framework for scalable digital development. The review indicates that trust is sustained through transparency, explainability, privacy protection, accountability, and continuous verification rather than through technical performance alone. It further demonstrates the need for sector specific governance, stronger technical safeguards, and future research focused on measurement, provenance, privacy enhancing technologies, and cross border data governance.

FUNDING

This review did not receive any specific grant from funding agencies in the public, commercial, or not for profit sectors. The work was completed independently by the author as part of a scholarly academic exercise.

ACKNOWLEDGMENT

The author acknowledges the valuable contributions of the researchers whose peer reviewed studies formed the basis of this review. Their work provided the evidence needed to synthesize the current understanding of digital trust in emerging technology ecosystems.

REFERENCES

1. Verhoef, P.C., T. Broekhuizen, Y. Bart, A. Bhattacharya, J.Q. Dong, N. Fabian and M. Haenlein, 2021. Digital transformation: A multidisciplinary reflection and research agenda. *J. Bus. Res.*, 122: 889-901.
2. Plekhanov, D., H. Franke and T.H. Netland, 2023. Digital transformation: A review and research agenda. *Eur. Manage. J.*, 41: 821-844.
3. Papagiannidis, E., P. Mikalef and K. Conboy, 2025. Responsible artificial intelligence governance: A review and research framework. *J. Strategic Inf. Syst.*, Vol. 34. 10.1016/j.jsis.2024.101885.
4. Otseje, I.J., O.A. Chinonso, D.C. Anih, U.M. Victoria, E.V. Chituru, O.A. Ogoh and O.O. Solaja, 2026. Auditing AI in finance: Risk, fairness, robustness and compliance: A systematic review. *Res. J. Inf. Technol.*, 18: 1-13.
5. Babel, M., L. Willburger, J. Lautenschlager, F. Völter and T. Guggenberger *et al.*, 2025. Self-sovereign identity and digital wallets. *Electron. Mark.*, 35: 2-14.
6. Sanner, T.A., A.M. Kempton, S. Russpatrick and J.I. Sæbø, 2025. Governing digital platform ecosystems for social options. *Inf. Syst. J.*, 35: 422-449.
7. Hassani, H., X. Huang and S. MacFeely, 2025. Mapping the evolution of data governance scientific research. *Data Policy*, Vol. 7. 10.1017/dap.2025.10014.
8. Andanda, P. and L. Mlotshwa, 2024. Streamlining the ethical-legal governance of cross-border health data sharing during global health emergencies. *Res. Ethics*, 20: 812-834.
9. Saveljeva, J. and T. Volkova, 2025. A survey on digital trust: Towards a validated definition. *Digital*, Vol. 5. 10.3390/digital5020014.
10. Oesterreich, T.D., E. Anton, F.M. Hettler and F. Teuteberg, 2024. What drives individuals' trusting intention in digital platforms? An exploratory meta-analysis. *Manage. Rev. Q.*, 75: 3615-3667.
11. Wanner, J., L.V. Herm, K. Heinrich and C. Janiesch, 2022. The effect of transparency and trust on intelligent system acceptance: Evidence from a user-based study. *Electron. Mark.*, 32: 2079-2102.
12. Steinbruch, F.K., L. da Silva Nascimento and D.C. de Menezes, 2022. The role of trust in innovation ecosystems. *J. Bus. Ind. Mark.*, 37: 195-208.
13. Fernández-Portillo, A., N. Ramos-Vecino, A. Ramos-Mariño and G. Cachón-Rodríguez, 2024. How the digital business ecosystem affects stakeholder satisfaction: Its impact on business performance. *Rev. Managerial Sci.*, 18: 2643-2662.

14. Faiz, F., V. Le and E.K. Masli, 2024. Determinants of digital technology adoption in innovative SMEs. *J. Innovation Knowl.*, Vol. 9. 10.1016/j.jik.2024.100610.
15. Tsai, M., S. Lee and S.W. Shieh, 2024. Strategy for implementing of zero trust architecture. *IEEE Trans. Rel.*, 73: 93-100.
16. Liu, C., R. Tan, Y. Wu, Y. Feng and Z. Jin *et al*, 2024. Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity*, Vol. 7. 10.1186/s42400-024-00212-0.
17. Glöckler, J., J. Sedlmeir, M. Frank and G. Fridgen, 2023. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Bus. Inf. Syst. Eng.*, 66: 421-440.
18. Ramamoorthi, K., V. Stamenova, R.H. Liu and O. Bhattacharyya, 2024. The implementation of federated digital identifiers in health care: Rapid review. *J. Med. Internet Res.*, Vol. 26. 10.2196/45751.
19. Liang, Z.Y., G.Y. Liu, Y. Ren, M. Yang, R.W. Jiang, Y. Luo and Y.S. Ma, 2025. Trustworthy data space collaborative trust mechanism driven by blockchain: Technology integration, cross-border governance, and standardization path. *Information*, Vol. 16. 10.3390/info16121066.
20. Feretzakis, G., K. Papaspyridis, A. Gkoulalas-Divanis and V.S. Verykios, 2024. Privacy-preserving techniques in generative AI and large Language Models: A Narrative Review. *Information*, Vol. 15. 10.3390/info15110697.
21. Polcumpally, A.T., K.K. Pandey, A. Kumar and A. Samadhiya, 2024. Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions. *Heliyon*, Vol. 10. 10.1016/j.heliyon.2024.e32975.
22. Lao, Y., N. Hirvonen and S. Larsson, 2025. AI and authenticity: Young people's practices of information credibility assessment of AI-generated video content. *J. Inf. Sci.*, 52: 975-989.
23. Azarov, A.A. and T.V. Tulupyeva, 2026. A model of digital trust in the context of the digitalization of society. *Pattern Recognit. Image Anal.*, 35: 1227-1231.
24. Glassberg, I., Y. Brender-Ilan and M. Zwilling, 2025. The key role of design and transparency in enhancing trust in AI-powered digital agents. *J. Innovation Knowl.*, Vol. 10. 10.1016/j.jik.2025.100770.
25. Đerić, E., D. Frank and M. Milković, 2025. Trust in generative AI tools: A comparative study of higher education students, teachers, and researchers. *Information*, Vol. 16. 10.3390/info16070622.
26. Fikardos, M., K. Lepenioti, D. Apostolou and G. Mentzas, 2025. Trustworthiness optimisation process: A methodology for assessing and enhancing trust in AI systems. *Electronics*, Vol. 14. 10.3390/electronics14071454.
27. Abomhara, M., L.O. Nweke, S.Y. Yayilgan, D. Comparin, K. Teyras and S. de Labriolle, 2024. Enhancing privacy protections in national identification systems: An examination of stakeholders' knowledge, attitudes, and practices of privacy by design. *Int. J. Inf. Secur.*, 23: 3665-3689.
28. Callo-Müller, M.V. and F. Sucker, 2026. Evolving approaches to cross-border data flows: Latin American and African perspectives. *Int. Data Privacy Law*, Vol. 16. 10.1093/idpl/ipaf037.
29. Zohaib, S.M., S.M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb and Z. Muhammad, 2024. Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. *Information*, Vol. 15. 10.3390/info15110734.
30. Schuetz, S., L. Kuai, M.C. Lacity and Z. Steelman, 2025. A qualitative systematic review of trust in technology. *J. Inf. Technol.*, 40: 55-76.
31. Arif, T., B. Jo and J.H. Park, 2025. A comprehensive survey of privacy-enhancing and trust-centric cloud-native security techniques against cyber threats. *Sensors*, Vol. 25. 10.3390/s25082350.
32. Feng, D., Y. Qin, W. Feng, W. Li, K. Shang and H. Ma, 2024. Survey of research on confidential computing. *IET Commun.*, 18: 535-556.
33. Sienkiewicz-Małyjurek, K. and B. Zyzak, 2025. Digital technologies in public administration networks: Systematic literature review and research avenues. *Adm. Soc.*, 57: 1051-1087.

34. Hariyani, D., P. Hariyani, S. Mishra and M.K. Sharma, 2025. A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices. *Green Technol. Sustainability*, Vol. 3. 10.1016/j.grets.2025.100169.
35. Cho, H., D. Froelicher, N. Dokmai, A. Nandi, S. Sadhuka, M.M. Hong and B. Berger, 2024. Privacy-enhancing technologies in biomedical data science. *Annu. Rev. Biomed. Data Sci.*, 7: 317-343.
36. Moreno, F.R., 2024. Generative AI and deepfakes: A human rights approach to tackling harmful content. *Int. Rev. Law Comput. Technol.*, 38: 297-326.
37. Klingbeil, A., C. Grützner and P. Schreck, 2024. Trust and reliance on AI - an experimental study on the extent and costs of overreliance on AI. *Comput. Hum. Behav.*, Vol. 160. 10.1016/j.chb.2024.108352.