CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Real-time data sharing frameworks – current state and research agenda
Authors	Sakhno, Anatoliy;Gewald, Heiko;Gupta, Ashish;Järveläinen, Jonna;Morgan, Lorraine;McCarthy, Stephen
Publication date	2026-09-01
Original Citation	Sakhno, A,, Gewald, H., Gupta, A., Järveläinen, J., Morgan, L. and McCarthy, S. (2026), 'Real-time data sharing frameworks – current state and research agenda', Communications of the Association for Information Systems, 59(1), 60 Available at: https://aisel.aisnet.org/cais/vol59/iss1/60/
Type of publication	Article (peer-reviewed)
Link to publisher's version	https://aisel.aisnet.org/cais/vol59/iss1/60
Rights	© 2026 AIS. This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Download date	2026-11-16 11:21:44
Item downloaded from	https://hdl.handle.net/10468/19416

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Communications of the Association for Information Systems

Volume 59 Paper in press

2026

Real-Time Data Sharing Frameworks – Current State and Research Agenda

Anatoliy Sakhno
University College Cork

Heiko Gewald
Neu-Ulm University of Applied Sciences

Ashish Gupta
Auburn University

Jonna Järveläinen
University of Jyväskylä

Stephen McCarthy
University College Cork

See next page for additional authors

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation

Sakhno, A., Gewald, H., Gupta, A., Järveläinen, J., McCarthy, S., & Morgan, L. (In press). Real-Time Data Sharing Frameworks – Current State and Research Agenda. *Communications of the Association for Information Systems*, *59*, pp-pp. Retrieved from https://aisel.aisnet.org/cais/vol59/iss1/60

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Real-Time Data Sharing Frameworks – Current State and Research Agenda

Authors

Anatoliy Sakhno, Heiko Gewald, Ashish Gupta, Jonna Järveläinen, Stephen McCarthy, and Lorraine Morgan

This article is available in Communications of the Association for Information Systems: https://aisel.aisnet.org/cais/vol59/iss1/60

Communications of the Association for Information Systems

Accepted Manuscript

Real-Time Data Sharing Frameworks – Current State and Research Agenda

Anatoliy Sakhno
University College Cork
0009-0007-6766-9971

Heiko Gewald
Neu-Ulm University of Applied Sciences
0000-0003-2107-2217

Ashish Gupta
Auburn University
0000-0003-4593-3261

Jonna Järveläinen
University of Jyväskylä
0000-0003-2032-489X

Stephen McCarthy
University College Cork
0000-0002-5761-7162

Lorraine Morgan
University of Galway
0000-0001-8344-1220

Please cite this article as: Sakhno, A., Gewald, H., Gupta, A., Järveläinen, J., McCarthy, S., & Morgan, L. (in press). Real-Time Data Sharing Frameworks – Current State and Research Agenda. *Communications of the Association for Information Systems.*

This is a PDF file of an unedited manuscript that has been accepted for publication in the *Communications of the Association for Information Systems*. We are providing this early version of the manuscript to allow for expedited dissemination to interested readers. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered, which could affect the content. All legal disclaimers that apply to the *Communications of the Association for Information Systems* pertain. For a definitive version of this work, please check for its appearance online at http://aisel.aisnet.org/cais/.

Communications of the Association for Information Systems

Panel Report ISSN: 1529-3181

Real-Time Data Sharing Frameworks – Current State and Research Agenda

Anatoliy Sakhno
University College Cork
0009-0007-6766-9971

Heiko Gewald
Neu-Ulm University of Applied Sciences
0000-0003-2107-2217

Ashish Gupta
Auburn University
0000-0003-4593-3261

Jonna Järveläinen
University of Jyväskylä
0000-0003-2032-489X

Stephen McCarthy
University College Cork
0000-0002-5761-7162

Lorraine Morgan
University of Galway
0000-0001-8344-1220

Abstract:

Real-time data sharing frameworks (RTDSFs) are emerging as vital digital infrastructures enabling low-latency, cross-organisational data flows in critical industries like finance, healthcare, or energy. Yet the governance, trust, and security challenges specific to real-time, automated, and multi-stakeholder contexts remain undertheorized in the Information Systems literature. This panel report synthesises discussion from an expert panel held at ECIS 2025 in Amman, Jordan, to develop a structured research agenda for the IS community. Through interpretive analysis of the panel transcript and contextual polling with eighteen participants, four interconnected pillars are proposed as productive sites of inquiry for RTDSFs — trust when action outruns validation, governance when oversight follows execution, federated intelligence as a redistribution of control under real-time conditions, and security collaboration under cascade risk and unequal preparedness. Polling results, offered here as indicative rather than confirmatory, suggested participant alignment on the primacy of enforceable governance and the need for regulatory engagement. The resulting research agenda identifies open questions, methodological pathways, and cross-pillar tensions specific to real-time, automated, and cross-organisational data sharing — positioning RTDSFs as a productive and underserved domain for IS inquiry.

Keywords: Real-Time Data Sharing (RTDS), Real Time Data Sharing Frameworks (RTDSFs), Digital Governance, Trust, Federated Machine Learning (FML), Cybersecurity.

[Department statements, if appropriate, will be added by the editors. Teaching cases and panel reports will have a statement, which is also added by the editors.]

[Note: this page has no footnotes.]

This manuscript underwent [editorial/peer] review. It was received xx/xx/20xx and was with the authors for XX months for XX revisions. [firstname lastname] served as Associate Editor.] **or** The Associate Editor chose to remain anonymous.]

1 Introduction

In an era of hyperconnected digital ecosystems, real-time data sharing is becoming a foundational infrastructure across key industrial sectors including financial services, healthcare, or energy. The exponential growth of Artificial Intelligence (AI) use cases further increases the need for high quality data exchanges, as with agentic AI automated algorithms take over tasks that were previously done by humans. Increasingly, decisions are automated, transactions are processed instantaneously, and operational risks are managed dynamically − all based on continuous data flows across organisational boundaries. Yet, as the pace and scale of data exchange intensifies, fundamental questions arise about control, accountability, and resilience of these mechanisms, that technical design alone cannot resolve.

Real-time data sharing frameworks (RTDSFs) are defined as socio-technical systems that enable continuous, low-latency exchange of digital information across organisational, sectoral, or jurisdictional boundaries (Kassem et al., 2020; Lovestone, 2020; He et al., 2025). Although they are technical backend infrastructures, they are so important for modern businesses that they are becoming deeply implicated in questions of power, privacy, cybersecurity, and regulation. For example, in financial services, Open Banking initiatives exemplify a shift from institution-centric to customer-centric models of data control. Consequently, this leads to questions of industry consolidation and platform dependencies (Zachariadis, 2020; Dinckol et al., 2023; Dezem et al., 2024). Similar dynamics are visible in healthcare, where interoperability architectures promise to integrate siloed patient data across care settings (Pflucke, 2025) with the vision of geographically distributed specialized care for a patient who is physically only in one place. Another example would be the energy industry, where AI-driven grid management platforms depend on real-time sensor streams but introduce novel cyber-physical vulnerabilities (Slate et al., 2024).

The promise of RTDSFs is accompanied by significant and undertheorized challenges. Cybersecurity vulnerabilities, from third-party Application Programming Interfaces (APIs) exposures to coordinated attacks on shared data hubs, are repeatedly flagged as critical risks in cross-organisational environments (Rabbani et al., 2024). More fundamentally, the speed of development in the RTDSFs space consistently outpaces the capacity of legal, ethical, and organisational safeguards to respond, creating conditions where automated decisions are executed before human oversight can intervene (Stahl, 2021; Markus and Rowe, 2023). These issues are specific to the real-time, automated, and cross-organisational character of RTDSFs, and they remain insufficiently addressed in the IS literature.

As RTDSFs become ever more embedded in critical public and private infrastructures, IS researchers are well positioned to examine the socio-technical configurations, governance models, and institutional logics that shape their development and consequences (Hossain et al., 2025). Yet the open questions specific to real-time, low-latency, and automated data-sharing contexts, how trust operates when action outruns validation, how governance functions when oversight follows execution, how control is redistributed when intelligence is federated, and how security is coordinated under cascade risk, have not been systematically addressed.

This panel report responds to that gap, following the structure and reporting conventions established for panel reports in CAIS (Wessel et al., 2021). It synthesises discussion from an expert panel convened at ECIS 2025 in Amman, Jordan, to propose a structured research agenda for the IS community. The panel brought together five researchers spanning finance, healthcare, energy, cybersecurity, and organisational governance, alongside an engaged audience of IS scholars. Sections 2 and 3 provide background on RTDSFs and the panel's organisation. Section 4 presents panellists' positioning statements. Section 5 synthesises four thematic pillars derived from the discussion. Section 6 develops these into a structured research agenda, including a cross-pillar analysis of tensions and interdependencies. Section 7 concludes with implications for IS research and practice.

2 Theoretical Foundations and Sectoral Variation

Building on the definition introduced in Section 1, RTDSFs allow entities to access, process, and act on data almost instantaneously, often within milliseconds, supporting decisions and operations that depend on current rather than historical information. While real-time data sharing is not new in high-frequency finance or logistics, recent advances in cloud infrastructure, APIs, and machine learning have expanded its use across healthcare, energy, and government services (Slate et al., 2024). Implementation varies by sector. In finance, Open Banking mandates real-time access to customer data, enabling third-party

service innovation (Dinckol et al., 2023). In energy, AI-driven platforms optimise grid operations through streaming sensor data (Slate et al., 2024). In healthcare, frameworks like the European Medical Information Framework (EMIF) enable distributed dataset access for pandemic response and safety surveillance (Lovestone, 2020).

RTDSFs depend on the interplay of regulatory mandates, governance frameworks, and trust mechanisms. Governance models range from centralised platform-based approaches, where a dominant actor coordinates standards and compliance, to distributed consortia that balance autonomy with coordination (Kassem, 2020; Zachariadis, 2020). In centralised models, efficiency may increase but dependency and reduced contestability become concerns. Distributed models require higher negotiation and interoperability. Trust is particularly critical in real-time contexts because data exchanges occur continuously and decisions are often automated, leaving little opportunity for human oversight or validation. Unlike traditional data-sharing environments where data quality can be verified before reuse, RTDSFs operate on streaming inputs that must be trusted and acted upon within milliseconds (Hossain et al., 2025). This immediacy shifts reliance toward systemic trust mechanisms such as cryptographic integrity checks, provenance metadata, and reputation-based access controls, complemented by procedural safeguards and transparency policies (Dantas, 2005).

Increasingly, RTDSFs are framed as critical digital infrastructures rather than standalone tools. This positions real-time data sharing as a public-private concern requiring sustained investment, resilience planning, and oversight (OECD, 2023). It demands alignment with broader socio-technical priorities such as inclusion, sustainability, and accountability, and challenges researchers to examine the power dynamics embedded in these systems' design and deployment (Stahl, 2021; Clemons et al., 2017). This infrastructural framing raises fundamental questions about control, accountability, and resilience that motivate the panel discussion and research agenda presented in subsequent sections.

Three theoretical traditions in IS are particularly generative for understanding RTDSFs, and this report draws on each as a lens for sharpening the research agenda. The first is socio-technical systems (STS) theory, which holds that effective information systems require the joint optimisation of technical and social subsystems (Bostrom and Heinen, 1977; Trist, 1981; Sarker et al., 2019). In classical STS thinking, both subsystems are designed together, with human roles, organisational structures, and technological architectures treated as mutually constitutive rather than sequentially determined. RTDSFs test this tradition in new ways. They span multiple organisations simultaneously, involve continuous rather than episodic data exchange, and include automated decision-making that operates at speeds beyond human deliberation. These conditions challenge the assumption that joint optimisation cannot be achieved only at the point of design. In RTDSFs, the social and technical subsystems are distributed across actors who may have conflicting interests, asymmetric capabilities, and no shared governance authority. STS theory thus remains relevant but requires extension to account for the cross-organisational, real-time, and automated character of these systems.

The second tradition is Carlile's knowledge boundaries framework, which identifies three types of boundaries in collaborative settings − syntactic, arising from differences in how information is encoded; semantic, from differences in how it is interpreted; and pragmatic, from differences in interests and power that make knowledge sharing politically contested (Carlile, 2002; Carlile, 2004; McCarthy et al., 2025). The panel discussion surfaced all three boundary types across the use cases examined. Technical interoperability challenges in the Anti-Money Laundering (AML) Bridge use case reflect syntactic boundary work. Disagreements over what patient data means across care settings in the Philips HealthSuite use case illustrate semantic boundaries. The competitive resistance to open-source solutions and the power asymmetries between large organisations and SMEs, evident in both the GridOS use case and a connected health case, reflect pragmatic boundaries in their most consequential form. All three use cases are examined in detail in Section 3.2. For RTDSFs, Carlile's framework highlights that the real challenge of cross-organisational data sharing is political as much as technical, with governance mechanisms needing to manage boundary conflicts on an ongoing basis rather than solely at the design stage.

The third tradition is inter-organisational systems (IOS) research, which has examined how shared digital infrastructures coordinate activity across organisational boundaries (Barrett and Konsynski, 1982; Reimers et al., 2014; Opriel et al., 2025). IOS research has documented how power asymmetries, lock-in effects, and governance failures shape the adoption and evolution of shared platforms, findings directly relevant to RTDSFs. More recently, digital platform governance research has extended this tradition to multi-sided markets and API-mediated ecosystems, examining how platform rules, data access policies, and regulatory mandates shape the balance of power between platform owners, contributors, and users

(Zachariadis, 2020; Dinckol et al., 2023; Yoo et al., 2024). RTDSFs share structural features with both IOS and digital platforms. They involve shared infrastructure, multi-party coordination, and contested governance but operate under real-time constraints and automation levels that existing IOS and platform governance research has not fully addressed. These three traditions collectively provide the theoretical vocabulary for the research agenda developed in Section 6, where each functions as an analytical lens for sharpening what is specifically unresolved in real-time, cross-organisational, and automated data-sharing contexts.

This report uses the term “frameworks” to describe RTDSFs while simultaneously characterising them as socio-technical systems. The choice is intentional. “Framework” emphasises the designed, governance-enabling dimension of RTDSFs. They are deliberately designed arrangements of rules, roles, standards, and infrastructure that coordinate how organisations interact across boundaries. “Socio-technical system” captures what RTDSFs become once realised − emergent, politically contested, and shaped by power dynamics that exceed their designers’ intentions. Both registers are necessary. The term “framework” directs attention to what can be designed and governed. “Socio-technical system” directs attention to what must be researched and understood. The tension between these two perspectives is itself productive, reflecting a broader pattern in IS where designed artefacts generate emergent social consequences that require ongoing theoretical and empirical attention.

3 Organization of the ECIS Panel

3.1 Panel Setup and Audience Engagement

The developments and challenges outlined above motivated a panel discussion at the European Conference of Information Systems 2025 in Amman, Jordan. The panel chair introduced the central theme “Who Holds the Power? Rethinking Data Sharing in Real-Time Ecosystems,” drawing on doctoral research focused on leveraging Open Banking, AI, and Federated Machine Learning (FML) to prevent money laundering and terrorist financing. To activate audience reflection, a live Vevox poll measured participants’ expertise in real-time data sharing frameworks and their perceptions of power dynamics. Eighteen participants engaged in the poll, establishing the topic’s relevance and anchoring the discussion in both practical and research-driven motivations.

The eighteen participants who engaged with the live polling were not formally profiled at registration. Based on the session context, an academic conference panel at ECIS 2025, the audience was predominantly drawn from the IS research community. The substantive nature of questions raised during the session, including challenges from senior scholars regarding trust barriers, competitive data-sharing concerns, and the structural risks of data breach between rival organisations, suggests an audience with both domain familiarity and research experience in related fields. Polling results are treated throughout this report as indicative of participant orientations rather than as a representative or confirmatory dataset.

The panel then transitioned to the panellists’ perspectives segment, where each speaker offered a short statement outlining their position, framed by their research profile. This surfaced the multiplicity of framings and underlying tensions shaping real-time data ecosystems. Rather than following a rigid sequence, panellists were encouraged to engage with each other’s ideas, sparking shared inquiry from the start.

3.2 Use Cases

Following this framing, the panel introduced three use cases to ground the conversation in practical examples:

- **AML Bridge (Finance):** An Estonian-origin platform now operating across twenty banks in the Baltics, Germany, and the United Kingdom, enabling real-time sharing of suspicion-led intelligence between financial institutions. Participating banks exchange encrypted, validated investigation cases and alerts through secure APIs, preserving data minimisation while enabling cross-institutional pattern detection. Initial case triage and alert routing are automated. Human investigators retain responsibility for escalation decisions. The operational impact is measurable − average investigation time fell from eighteen to three minutes following deployment, a sixfold improvement over sequential, siloed investigation cycles (cf. Jackson, 2014).

- **Philips HealthSuite (Healthcare):** A cloud-based platform integrating real-time data flows from electronic medical records, laboratory systems, medical imaging, telehealth services, and home monitoring devices into a unified patient view. HealthSuite Edge, a managed Virtual Private Network (VPN) service, bridges local hospital networks to the central cloud environment. Alert generation, triage prioritisation, and operational scheduling are increasingly automated. Diagnostic and treatment decisions remain human-in-the-loop. The governance challenge is acute − patient consent frameworks, data minimisation requirements, and cross-jurisdictional privacy regulations must be enforced continuously across a multi-party ecosystem where data provenance and access rights are constantly changing (cf. Knoppers, 2014).

- **GE Vernova GridOS (Energy):** An enterprise grid orchestration platform unifying IT and operational technology data to manage decentralised energy networks in real time. Data flows include sensor readings from distributed energy resources, grid stability measurements, weather analytics for dynamic line rating, and remote sensing data for infrastructure hazard detection. Load balancing, outage restoration, renewable dispatch, and real-time line capacity adjustments are substantially automated; human operators retain supervisory oversight but cannot intervene at the millisecond timescales at which grid decisions execute. Zero-trust security is architecturally embedded in alignment with the National Institute of Standards and Technology (NIST) Special Publication 800-207 zero-trust architecture standard. This supports compliance with mandatory North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) requirements, reflecting that a security failure at any node can propagate to system-wide instability before any contractual or regulatory safeguard can respond**.**

These examples illustrated how pioneer real-time data sharing initiatives manifest in practice, revealing both their transformative potential and the governance and trust challenges involved.

3.3 Panel Discussion Structure

The panel was then structured around three thematic discussions, each lasting 15 minutes with active audience engagement:

1. **Designing Adaptable Frameworks:** Strategies for designing data-sharing frameworks that are adaptable across regulatory regimes, sectors, and organisational boundaries.
2. **Transparency, Collaboration, and Innovation:** How transparency mechanisms can be designed without exposing sensitive information or weakening competitive advantages, and the role of collaboration between regulators, platforms, and innovators.
3. **Addressing Risks and Cybersecurity Threats:** Risk management and cybersecurity as foundational to trust, including emerging threats in real-time infrastructures and the tension between speed and security.

A closing Vevox poll invited participants to reflect on how their perceptions of trust had shifted and to identify which factors they now considered most critical for sustainable real-time data sharing, as well as which stakeholder groups should play a stronger role in shaping these ecosystems.

Throughout the panel, active use of live polling and targeted facilitation engaged the audience as active participants in shaping the discussion. The panel chair's dual role as researcher and Product Manager enabled bridging academic inquiry with industry practice. The panel was recorded and transcribed for subsequent analysis.

In the following sections, we present initial position statements from each panellist, synthesise the main discussion threads into four themes, and conclude with integrative takeaways and panellists' reflections.

3.4 Data Analysis Approach

The four pillars presented in this report were derived through an interpretive synthesis of the panel's recorded and transcribed proceedings (cf. Braun and Clarke, 2006). Following the panel session at ECIS 2025, the first author conducted a systematic review of the full transcript, undertaking approximately five iterative passes through the material. Each pass was oriented toward identifying recurring themes, areas of convergence and tension, and the concepts that panellists returned to most consistently across discussion segments and audience exchanges.

The analytical process was interpretive rather than deductively coded. Rather than applying a predetermined coding scheme, the approach drew on the thematic concerns surfaced by panellists in their positioning statements, their responses to facilitated questions, and their engagement with audience polling results. Candidate themes were progressively consolidated into higher-order constructs, with the four pillars emerging as the most robust and conceptually distinct clusters that spanned multiple discussion segments and sectoral contexts.

The derived pillars were subsequently shared with all co-authors for review and feedback. Co-authors confirmed the representativeness of the pillars relative to their own contributions and provided supplementary perspectives that refined the characterisation of each pillar. This member-checking step lends additional credibility to the synthesis, though the analysis remains interpretive and panel-derived rather than a systematic empirical study.

The live polling data from the eighteen audience participants, drawn predominantly from the academic IS community, are treated throughout this report as indicative and contextual. They illuminate participant orientations at a moment in time and provide a suggestive signal regarding perceived priorities. They do not constitute a statistically representative dataset. To protect anonymity, audience members were not formally profiled, though the session's registration context and the nature of questions raised suggest a predominantly research-oriented audience with domain familiarity.

Where panellist contributions are quoted in this report, all quotations are drawn from the recorded and transcribed panel proceedings. Where the quoted speaker is also a co-author of this manuscript, the quotation represents their contribution to the panel discussion rather than to the manuscript itself, and is treated as primary panel data on the same basis as contributions from other participants. To preserve transparency, all such quotations are attributed to the speaker and their institutional affiliation.

4 Initial Positioning Statements

At the beginning of the panel, each panellist articulated their position on real-time data sharing frameworks in increasingly interconnected digital ecosystems.

Ashish Gupta (Auburn University): My perspective on real-time data sharing is grounded in research across high-frequency trading, fraud detection, and autonomous systems. In these contexts, "real-time" is inherently relative − in capital markets, delays of even 0.5 seconds can be critical, prompting firms to co-locate infrastructure near data towers. Time functions as a critical dependency in this environment. Vulnerabilities like time drift or lag manipulation can have systemic implications. Traditional real-time frameworks rely on centralised raw data sharing, presenting privacy, scalability, and trust challenges. We have explored FML as an alternative, where local models are trained on private data and only model parameters are shared centrally. This approach preserves privacy, improves model performance iteratively, and offers a viable path forward for scalable, privacy-conscious real-time data sharing architectures.

Heiko Gewald (Neu-Ulm University of Applied Sciences): My perspective stems from research into digital transformation in healthcare, an industry with immense potential but severe underdevelopment in data sharing. The COVID-19 pandemic painfully illustrated this gap in Germany. Case numbers were often transmitted via fax, with delays of hours or days. Structured and timely data sharing could unlock major advances in cancer treatment, AI-driven documentation, and personalised drug development, yet deep ethical, technical, and governance concerns persist. Medical data is uniquely sensitive and valuable. Full medical records are worth hundreds of dollars on the dark. Researchers can offer technical approaches like anonymisation and differential privacy, but only strong policy leadership can create conditions for responsible and useful data sharing (cf. Modi et al., 2023). Until political will and public trust align, healthcare will remain far from the real-time frontier, even though such capabilities could benefit the patients and redefine crisis management.

Jonna Järveläinen (University of Jyväskylä): My work explores cybersecurity in networks spanning critical infrastructure such as energy grids, ports, and automated mining equipment, in which real-time data-sharing is central for the networks. In these environments, data may not be highly sensitive, yet any interruption is ruinously expensive. A brief halt in a diamond-mine operations or in an energy grid can cost millions. Current governance frameworks overlook multi-stakeholder ecosystems where several partners must exchange low-latency data seamlessly. Our field studies show that small and medium-sized enterprises (SMEs) often lag in cybersecurity maturity, heightening supply-chain attack risks. Once one

node is compromised, malware can ripple across the network long before contractual arrangements can respond. We have studied multi-stakeholder security-governance models stressing pre-incident trust-building − shared playbooks, joint exercises, and continuous knowledge exchange among partners of unequal size. Without collective trust architectures, real-time data-sharing frameworks rest on fragile foundations.

Stephen McCarthy (University College Cork): My work examines the interplay between technical interoperability and organisational coordination in real-time data-sharing ecosystems. While recent advances in APIs and modular architectures have lowered technical barriers, seamless data sharing remains as much a governance challenge as a design one. Drawing on Carlile's knowledge boundaries framework, I show that data transfer is syntactic, semantic, and − just as fundamentally − political, shaped by power, trust, control, and competing interests. These political boundaries become most visible in multi-organisational settings where actors vary in size, intellectual property ownership, and digital maturity. In one healthcare project involving connected devices, the multinational firm resisted open-source solutions due to competitive concerns, while the startup advocated for openness. This underscores the need for governance design that accounts for different forms of control, centralised, decentralised, or emergent, and the nature of relationships, whether contractual or trust-based.

Lorraine Morgan (University of Galway): Drawing on research into Inner Source, adopting open-source principles inside organisations, I argue that Inner Source culture can transform real-time data-sharing frameworks. By exposing code, data models, APIs, and documentation internally, companies shift from siloed development to transparent, collaborative ecosystems. Our longitudinal studies of Zalando, Philips Healthcare, and PayPal show a repeatable four-stage pathway: capture reusable components, reuse them across teams, share them organisation-wide, and open selected assets to external partners. Each stage tightens feedback loops and scales modular building blocks that underpin low-latency data exchange. Inner Source allows decentralised data ownership to coexist with central governance, ensuring both flexibility and compliance. However, Inner Source succeeds only when governance structures reward contribution, trusted committers safeguard quality, and leadership signals that transparency matters more than guarding ownership.

5 Four Pillars for Real-Time Data Sharing Frameworks in the IS Field

The positioning statements presented above reveal both the complexity and the convergence underlying real-time data sharing frameworks across sectors. While each panellist brought distinct contextual lenses their contributions revealed shared foundational concerns.

Through iterative analysis of the panel discussions, polling data, and interactive exchanges, four interconnected pillars emerged as productive sites of inquiry for sustainable RTDS implementation: ***Mutual Trust, Transparent Governance, Federated Intelligence and Security Collaboration***. These pillars go beyond technical specifications or policy recommendations. They represent the socio-technical conditions that must be simultaneously addressed for RTDS frameworks to achieve both operational effectiveness and societal legitimacy.

The following analysis examines each pillar through the grounded perspectives offered by panellists, synthesizing their insights with broader empirical evidence to illuminate both the challenges and pathways forward for RTDSFs development.

5.1 Mutual Trust

Trust was recognized as the cornerstone enabling real-time data sharing, particularly in sensitive domains like healthcare and finance. Professor Heiko Gewald led this discussion by emphasising that while the technical and ethical risks of data sharing are real, they must be managed rather than avoided. In his positioning statement, Professor Gewald argued that large-scale, system-wide sharing of patient data is not optional but inevitable:

> *"I have difficulties envisioning a world where we do not share much more medical data as we do today."*

Drawing on examples from the healthcare domain, Professor Gewald illustrated how data already holds transformative potential. He referred to a case where hospital-wide big data analytics of previous patients revealed undiagnosed type 2 diabetes in patients presenting with other medical issues. This, he suggested, is a small glimpse into what could be achieved if trust-based sharing becomes the norm.

Similar cases have demonstrated the value of federated, privacy-preserving analytics in healthcare, especially under frameworks like Enabling Personalised Intervention (EPI), which align policy, technical feasibility, and stakeholder trust (Kassem et al., 2020; cf. Modi et al., 2023).

As Professor Gewald established in his positioning statement, healthcare data sharing faces unique ethical and technical barriers. Sensitive data, such as mental health records or sexually transmitted diseases, raises critical questions about who should have access and under what conditions. Even anonymisation, often proposed as a solution, presents a paradox. It protects individuals but can hinder follow-up actions when someone's life is at stake. As Professor Gewald observed during the panel:

> *"If in that anonymised data set you find a person who is critically ill, and you cannot get in touch with that person."*

To this end, Professor Gewald underscored the need for robust data governance, designed with patients' rights at the centre, yet flexible enough to enable urgent, real-time decisions (cf. Knoppers, 2014). He noted Germany's transition to an electronic patient record system, in which the individual is nominally in control of their own data. Yet even this model faces challenges. What happens when a patient lacks the cognitive capacity to grant access, or when real-time access is needed in an emergency?

Other panellists added complementary perspectives. Ashish Gupta emphasised the regulatory complexity and technical constraints of real-time data use in healthcare, particularly in the US context. Despite holding data sharing agreements with medical institutions, he noted the difficulty in accessing patient-specific information under Health Insurance Portability and Accountability Act (HIPAA) regulation. These issues are echoed globally, where privacy and legal compliance frameworks often clash with the operational need for timely access (Panhuis et al., 2014; Pflucke, 2025).

Jonna Järveläinen further elaborated that trust must precede any cybersecurity collaboration. Drawing on her organisational-level research, she argued that security mechanisms cannot compensate for a lack of trust among stakeholders. Instead, preparing for incidents before they occur requires long-term collaboration, joint exercises, information sharing, and governance structures. She also cautioned that even when patients are legally in control of their data, as in Finland, the real power often lies with system providers, who design and operate the platforms (Koskinen and Kimppa, 2016). Similar tensions between user control and system-level governance have been noted in the EMIF project, where technical interoperability and ethical safeguards were critical enablers of trust across diverse datasets and jurisdictions (Lovestone, 2020).

From a governance standpoint, Professor Gewald concluded that regulatory action is indispensable. Researchers can design frameworks, but without political will and enforcement, responsible data sharing at scale will remain aspirational. At the same time, willingness to share must be cultivated among institutions, professionals, and the public if trust is to take root at scale.

In sum, this session clarified that trust is not a soft value but a structural prerequisite for sustainable RTDSFs. Without it, even the most advanced technical architectures will fail to gain traction. But with it, data sharing can become a vehicle for societal benefit − one that is real-time, responsible, and resilient.

5.2 Transparent Governance

Transparent and enforceable governance was identified by both panellists and the audience as a critical enabler for sustainable real-time data sharing. Indicatively, 67% of audience participants ranked it as the most important factor, above technical architecture, security mechanisms, or stakeholder trust, though this reflects the orientations of a small, predominantly academic audience rather than a representative sample.

Dr. Stephen McCarthy positioned this topic within the broader field of information systems, calling attention to the need for socio-technical governance models. He argued that emerging technologies, especially agentic AI and autonomous systems, are intensifying the demand for frameworks that do more than offer technical guidance. According to McCarthy, future RTDS initiatives require both transparent governance structures and social coordination mechanisms for regulatory enforcement. As Dr McCarthy noted during the panel discussion:

> *"It's socio-technical. We need to understand both. Otherwise, we will end up with systems that not fully fit for purpose."*

His emphasis carried practical urgency. Dr. McCarthy pointed to the rising complexity of digital infrastructures and the blurred boundaries between technical autonomy and human oversight. These

developments call for a new generation of governance research that takes seriously the integration of legal, ethical, and operational enforceability from the outset. Similar calls for coordinated, enforceable frameworks have emerged in open finance and RegTech domains, where real-time access to sensitive data requires layered safeguards, legal mandates, and reciprocal trust between actors (Grassi and Lanfranchi, 2022; OECD, 2023).

This view was further contextualised by a live poll during the panel, in which approximately two-thirds of participants identified government and regulators as the primary actors to lead RTDS ecosystems forward − a suggestive rather than definitive signal given the audience size. While innovation may originate from industry, the panel agreed that policy must "make it happen," particularly in sectors like healthcare and finance where personal data is highly sensitive. As recent studies on the UK's Open Banking ecosystem have shown, policy-led governance is vital for standardisation, interoperability, and sustained innovation (Dinckol et al., 2023).

Other panellists echoed this view. Professor Heiko Gewald stressed the urgency of regulatory clarity to support real-time medical data sharing. In his example, anonymisation may be legally compliant but practically dangerous when follow-up care is needed. He argued for governance systems that balance privacy with ethical responsibility, particularly in life-critical contexts. This reflects broader findings in healthcare data infrastructures, where transparency without enforceable protocols has led to fragmentation and hesitation among stakeholders (Kassem et al., 2020).

Professor Ashish Gupta highlighted the cost and complexity of RTDS infrastructure, especially for AI training. He noted that without clearly defined regulatory roles and responsibilities, many institutions are hesitant to commit to large-scale deployments. As Professor Gupta asked during the panel: *"Who is going to own the data, the security, the regulation?"* − a governance question at its core.

Dr. Jonna Järveläinen brought attention to the interdependence of governance and cybersecurity, arguing that security controls must be designed within enforceable frameworks rather than applied retroactively. She warned that governance without enforcement is unlikely to resolve real-world risks such as system availability or provider liability. The experience in private-sector data sharing supports this, where lack of enforceable governance remains one of the chief barriers to broader cooperation (Fassnacht et al., 2023).

Taken together, the discussion converged on a clear conclusion − transparent governance alone is insufficient without the capacity to enforce rules across complex stakeholder networks. This includes legal enforceability, platform accountability, and the institutional will to intervene when necessary.

For IS scholars, Dr. McCarthy concluded, this represents both a challenge and an opportunity. The governance of RTDS extends beyond a policy problem into a core research agenda that calls for theory-informed, empirically grounded, and practice-ready solutions.

5.3 Federated Intelligence

Professor Gupta elaborated on the FML approach he introduced in his positioning statement, emphasizing that this architecture can enable real-time data sharing without compromising data sovereignty or privacy. Professor Ashish Gupta led this part of the discussion, outlining both the strategic value and the substantial challenges of deploying FML in domains like healthcare and financial services.

Professor Gupta positioned FML as a crucial enabler of next-generation AI models, particularly when access to real-time, high-quality data across multiple stakeholders is needed. In this model, data remains distributed at local nodes (e.g. hospitals, banks), while only model updates, not raw patient or customer data, are shared and aggregated centrally. This approach enhances privacy while still allowing for robust AI training. Such decentralised models are increasingly being explored in sensitive sectors as a solution to reconcile privacy regulation with data-driven innovation (OECD, 2023; Pflucke, 2025). In his panel contribution, Professor Gupta noted:

> *"Real-time data sharing has tremendous value, especially for developing next-generation AI models using concepts like federated machine learning. But there has to be a strong reason to do this. It is costly and requires significant infrastructure."*

He emphasised that such deployments are not yet mainstream due to high operational and capital costs, especially around infrastructure and data security. Although cloud-based environments offer partial solutions, Professor Gupta warned that the governance of data ownership, privacy, and regulation must be clearly defined before FML can be scaled. Industry studies echo this challenge, noting that even in

highly regulated environments like banking, FML requires foundational changes to system design, trust frameworks, and stakeholder alignment (Grassi and Lanfranchi, 2022; Dezem et al., 2024).

The discussion acknowledged that FML presents a technically viable but socio-politically complex architecture. Even if the technical architecture is in place, real-time collaboration across organisations remains difficult without enforceable governance, role clarity, and trust. A systematic review of data-sharing challenges among private organisations has shown that lack of mutual trust and role standardisation are persistent barriers, even when technical solutions exist (Fassnacht et al., 2023).

Professor Gupta also pointed to validated real-time analytics frameworks, including approaches to misinformation detection, as evidence that real-time analytical architectures can be made operationally robust when use cases are clearly defined (Zhang et al., 2023).

Professor Heiko Gewald offered a more optimistic view:

> *"I'm a strong believer that our computing power will be much higher and much cheaper. Real-time should not be much of an issue in 10 to 15 years."*

However, Professor Gupta emphasized the need to align infrastructure readiness with regulatory support and institutional willingness to share data at scale. He argued that real-time architectures must be justified by real-time needs, particularly when used in AI applications that directly impact human health or financial decision-making. Regulatory guidance in this space is still evolving, and until clear standards and accountability frameworks are in place, FML may remain confined to experimental or pilot phases (Pflucke, 2025).

Dr. Jonna Järveläinen added that FML may also enhance resilience and mitigate cybersecurity risks. By keeping data decentralised, the attack surface is distributed, and it is unlikely that a single provider becomes a systemic point of failure. Recent work in AI governance has highlighted that resilience and explainability are just as important as efficiency when deploying AI for critical infrastructure (Slate et al., 2024).

In sum, the panel recognised FML as a high-potential yet high-cost innovation solution. It offers a reference architecture for RTDS that meets both ethical and analytical demands but only if it is supported by enforceable governance, shared responsibilities, and meaningful institutional buy-in.

5.4. Security Collaboration

Multi-stakeholder collaboration was identified as a necessary precondition for managing security risks in real-time data sharing ecosystems. Expanding on earlier discussions of cross-sector coordination, Dr. Järveläinen emphasized that cybersecurity requires a shared organisational responsibility that demands proactive coordination among all stakeholders involved.

She stressed that, within the classic confidentiality-integrity-availability security triad, availability emerges as the most critical aspect in RTDS, especially in time-sensitive environments such as healthcare. In these settings, even minimal data lags, measured in milliseconds, can delay life-saving decisions. For instance, a system failure that prevents a surgeon from seeing a patient's allergy record prior to surgery could have fatal consequences. As Dr. Järveläinen noted in the panel discussion:

> *"In real-time data sharing, availability becomes the most pressing cybersecurity risk. Even milliseconds matter, especially in healthcare where missing data can cost lives."*

Dr. Järveläinen argued that cybersecurity needs to be embedded into the architecture and governance of data sharing platforms from the start, not added as an afterthought. She highlighted that while the privacy of financial and healthcare data remains vital, system reliability and continuity of access are paramount when real-time operations are at stake. These insights are supported by broader research emphasising that AI and data systems in critical infrastructure must prioritise trustworthiness, resilience, and explainability (Slate et al., 2024).

She also called for greater distribution of system responsibilities to reduce systemic risks. Although she did not explicitly endorse blockchain, she supported the idea of decentralised architectures that would avoid placing control and failure risk into the hands of a single authority. In her panel contribution, Dr Järveläinen argued:

> *"Some kind of distributed systems might be useful. Not everything should be held by one single provider."*

This perspective aligns with emerging governance models in both public and private sectors, where decentralised and interoperable infrastructures are increasingly seen as necessary for both innovation and security (Grassi and Lanfranchi, 2022; Dinckol et al., 2023). Studies in RegTech and open finance confirm that shared control models can distribute risk more effectively and build systemic resilience.

This insight aligns with a broader theme in the panel that collaboration among stakeholders is not a soft ideal but a structural necessity. Real-time security cannot be achieved through isolated controls. It requires shared protocols, cross-institutional rehearsals, mutual agreements, and clarity on incident response. Empirical studies have shown that collaborative cybersecurity ecosystems are more effective when supported by defined governance mechanisms, simulation exercises, and regulatory incentives (Fassnacht et al., 2023).

Professor Ashish Gupta supported this view by noting the complex dependencies and potential vulnerabilities that arise when multiple institutions engage in RTDS. He echoed the need for role clarity in governance and argued that without strong collaboration, even the best federated architectures could fail under attack.

Dr. Stephen McCarthy added that socio-technical integration must support any collaboration strategy. Systems are no longer neutral platforms. They embody value-laden decisions, underlying assumptions, and commercial priorities that affect human lives. Therefore, governance and security must be co-designed, not separated, a principle echoed in current regulatory discussions on AI accountability (Pflucke, 2025).

In closing, Dr. Järveläinen emphasised that the real challenge is not the lack of technological options but the lack of collective preparedness. Effective collaboration, she argued, must precede crises, not emerge from them. Without structured, enforceable partnerships between healthcare providers, data platforms, cybersecurity actors, and regulators, the vision of secure RTDS will remain aspirational. As Dr. Järveläinen concluded during the panel:

> *"Of course, there is hope but we need collaboration. Whether we are talking about innovation or risk, we must act together."*

Building on these panel-derived perspectives, we now turn to a structured research agenda that operationalizes the four pillars identified above.

6 Research Agenda for RTDSFs

This section compiles a structured research agenda for RTDSFs intended to guide future IS research. It addresses open research problems that arise when trusted and transparent data sharing must operate under real-time, cross-organisational conditions.

The following subsections examine each of the four research agenda pillars identified by the panel: (1) *Mutual Trust under conditions of speed and automation*, (2) *Transparent Governance beyond visibility and disclosure*, (3) *Federated Intelligence as a redistribution of control*, and (4) *Security Collaboration as a collective action problem*. Each subsection frames the core research challenge and is accompanied by a focused research agenda table that specifies the underlying knowledge gap, exemplary research questions, useful methodological approaches, as well as the envisioned theoretical and practical contributions. In subsection 6.5 we analyse the interdependencies between the four pillars, while Subsection 6.6 returns to panellist reflections grounding the agenda in practitioner perspectives.

6.1 Mutual Trust under Conditions of Speed and Automation

Across domains, the panel discussion revealed that mutual trust, the reciprocal confidence among participating organisations that shared data will be handled with integrity, that governance arrangements will be honoured, and that risks and responsibilities will be distributed equitably, cannot be treated as a stable precondition or a gradually accumulated relational asset in RTDSFs (van Panhuis et al., 2014; Fassnacht et al., 2023). Instead, trust increasingly operates under conditions where data must be acted upon immediately, often without the possibility of prior validation or timely human intervention. Grounded in role clarity, aligned incentives, and reliable information flows, trust shifts from a deliberative judgment into a systemic dependency, embedded in architectures, protocols, and automated decision routines (Dantas and Dalziell, 2005; Dezem et al., 2024). As a result, breakdowns of trust may occur after

consequential actions have already been taken, raising questions about reversibility, responsibility, and recovery that are largely absent from existing theories of IS.

For IS researchers, this reframing suggests that trust in RTDSFs is less about willingness to share and more about exposure to irreversible consequences (Table 1). Trust becomes entangled with asymmetries in technical capability, regulatory protection, and decision authority, particularly in cross-organisational settings. This calls for research that examines trust as a temporal and infrastructural phenomenon, shaped by automation, latency, and systemic interdependence, alongside its more familiar treatment as a psychological or institutional construct.

Table 1. Research Agenda for Mutual Trust in RTDSFs

Theme	**Description**
Core Tension / Knowledge Gap	Existing IS trust theories are largely built on assumptions that do not hold in real-time, automated, and cross-organisational environments. They presuppose identifiable actors, episodic exchanges, and meaningful opportunities for prior validation or ex-post accountability (Dantas and Dalziell, 2005; Fassnacht et al., 2023). In RTDSFs, however, data is exchanged continuously, decisions are automated, and validation frequently occurs after consequential action has already been taken (Dantas and Dalziell, 2005; Dezem et al., 2024). This creates conditions in which breakdowns of trust may be discovered only once irreversible outcomes have been produced, and where recovery, reversibility, and responsibility are difficult to assign. The core unresolved question is not whether organisations are willing to share data, but whether trust can be established and sustained when speed and automation structurally reduce opportunities for deliberation, oversight, and cross-organisational negotiation − particularly when participants differ significantly in technical capability, regulatory protection, and decision authority (van Panhuis et al., 2014; Fassnacht et al., 2023; Dezem et al., 2024).
Research Questions	• How does trust formation differ when data must be acted upon in real-time rather than validated before use? • Under what conditions does automation substitute for, undermine, or reconfigure trust in RTDSFs? • How do asymmetries shape trust relationships among RTDSF participants? • What recovery mechanisms are feasible after automated decisions are executed?
Methodological Approaches	• Systematic literature reviews mapping trust barriers (van Panhuis et al., 2014; Fassnacht et al., 2023) • Case studies eliciting trust dependencies (Dantas and Dalziell, 2005) • Multiple-criteria decision analysis with evidential reasoning (Dezem et al., 2024)
Anticipated Contributions	**Theoretical:** Extensions of theories of IS trust for temporal constraints, automation-mediated trust, and distributed accountability. **Practical:** Trust design playbooks: information flow alignment, role clarity, reciprocity mechanisms, multi-stakeholder negotiation frameworks.
Value Propositions for IS Communities	**Socio-technical IS:** Trust models embedded in routines and infrastructure. **Trust and control studies:** Trust/control trade-offs when validation lags action. **Behavioural IS:** Automation-mediated trust in high-stakes environments.

6.2 Transparent Governance beyond Visibility and Disclosure

The panel highlighted that transparent governance, the institutional capacity to make data access rights, decision rules, and accountability arrangements explicit, enforceable, and subject to ongoing regulatory stewardship across participating organisations, takes on a more ambiguous role in real-time data sharing environments (Dinckol et al., 2023; OECD, 2023; Pflucke, 2025). In RTDSFs, governance processes often lag behind automated execution, meaning that visibility into decisions may arrive too late to enable meaningful oversight or contestation. Moreover, increased transparency can introduce new risks, such as exposing sensitive operational details, amplifying strategic behaviour, or obscuring accountability when decision-making is distributed across technical and organisational layers (Zachariadis, 2020; Grassi and Lanfranchi, 2022).

These dynamics suggest that governance in RTDSFs cannot be reduced to making rules or processes more visible. Instead, governance becomes a question of when and where control is exercised, and by whom, under conditions of speed and cross-jurisdictional complexity (Dinckol et al., 2023; Pflucke, 2025). For IS scholars, this opens a research agenda focused on how governance architectures redistribute power over time, how enforceability is achieved when actions precede oversight, and how accountability can be meaningfully assigned in environments characterised by automated, real-time coordination (Zachariadis, 2020; OECD, 2023) (Table 2).

Table 2. Research Agenda for Transparent Governance in RTDSFs

Theme	**Description**
Core Tension / Knowledge Gap	Prevailing IS governance models are designed for contexts in which decision rights are stable, accountability mechanisms are identifiable, and governance processes unfold over time with opportunities for deliberation and correction (Zachariadis, 2020; Dinckol et al., 2023). RTDSFs challenge each of these assumptions simultaneously. Governance must operate across continuous data flows, automated execution, and multi-jurisdictional participation, yet the actors, standards, and enforcement mechanisms needed to make this work remain contested and unevenly developed (OECD, 2023; Pflucke, 2025). Transparency is frequently invoked as the solution, but in real-time settings it introduces its own complications. Visibility into system behaviour may arrive too late to enable meaningful oversight, disclosure of operational details may expose strategic vulnerabilities or compromise security, and distributing decision-making across technical and organisational layers can obscure rather than clarify accountability (Grassi and Lanfranchi, 2022; Pflucke, 2025). The core unresolved challenge is therefore not how to make RTDSFs more visible, but how governance can be designed to be enforceable and accountable when oversight structurally follows execution rather than preceding it (Zachariadis, 2020; Dinckol et al., 2023; OECD, 2023).
Research Questions	• How does governance function when decisions are executed automatically before oversight is possible? • Under what conditions does transparency enhance accountability in RTDSFs? • How are decision rights, liabilities, and responsibilities negotiated across organizational and regulatory boundaries? • How do different governance architectures redistribute power among RTDSF participants over time?
Methodological Approaches	• Longitudinal qualitative studies using interviews, document analysis, and process tracing (Dinckol et al., 2023) • Legal analysis examining data access rights and liability allocation (Pflucke, 2025) • Comparative policy analysis (OECD, 2023) • Systematic review with bibliometric analysis (Grassi and Lanfranchi, 2022) • Conceptual analysis of APIs as boundary resources (Zachariadis, 2020)
Anticipated Contributions	**Theoretical:** Frameworks linking transparency to enforceable rights, continuous oversight, and machine-readable regulation.

	Practical: Governance design patterns: regulatory stewardship models, API standardization playbooks, liability frameworks, consent architectures, RegTech-enabled compliance.
Value Propositions for IS Communities	**Digital governance/policy IS:** Governance-by-design frameworks; regulatory stewardship models. **Socio-technical systems:** APIs as boundary resources operationalizing governance. **Regulation:** RegTech for operational transparency. **Critical IS:** Power distribution analysis.

6.3 Federated Intelligence as a Redistribution of Control

Discussions around federated intelligence, the capacity to generate coordinated analytical outputs across multiple autonomous participants without centralising raw data, by distributing computation, model training, and decision logic across organisational and infrastructural boundaries, underscore that decentralising computation does not eliminate governance or trust challenges but rather relocates them (Javan et al., 2024; Rabbani et al., 2024; Slate et al., 2024). While federated approaches promise to reconcile real-time analytics with privacy and data sovereignty, they also introduce new layers of dependency. Control over model aggregation, parameter updates, and infrastructural coordination may become concentrated in ways that are less visible to individual participants, particularly when models evolve continuously and autonomously (Dezem et al., 2024; Rabbani et al., 2024).

From an IS perspective, federated intelligence reframes architecture as a site where power and accountability are negotiated rather than technically resolved (Table 3). The shift from data sharing to model sharing raises questions about who can explain, contest, or intervene in real-time decisions, especially when no single actor has full visibility into the system's behaviour (Javan et al., 2024; Slate et al., 2024). This tension positions federated intelligence as a fertile ground for research at the intersection of design science, governance, and socio-technical analysis (Dezem et al., 2024; Rabbani et al., 2024).

Table 3. Research Agenda for Federated Intelligence in RTDSFs

Theme	Description
Core Tension / Knowledge Gap	Federated and decentralised intelligence architectures are increasingly presented as a means of reconciling the demands of real-time analytics with privacy, data sovereignty, and regulatory constraints − enabling collaboration without requiring the pooling of raw data (Rabbani et al., 2024; Slate et al., 2024). This framing, however, obscures an important shift: distributing computation rather than data does not eliminate questions of control and accountability, but reconfigures them in ways that are less visible and less well understood (Dezem et al., 2024; Rabbani et al., 2024). In RTDSFs, where models evolve continuously and decisions may be executed automatically before any single actor has reviewed the underlying logic, it remains unclear who is responsible for outcomes, who can explain or contest a decision, and how governance is enacted across organisational and jurisdictional boundaries (Javan et al., 2024; Slate et al., 2024). The core unresolved question is not whether federated intelligence is technically viable, but whether distributing intelligence under real-time conditions creates new concentrations of power, particularly at the model aggregation layer, that undermine the accountability and transparency that governance frameworks are meant to ensure (Dezem et al., 2024; Rabbani et al., 2024; Slate et al., 2024).
Research Questions	• How does intelligence distribution alter accountability when real-time decisions are based on updated, federated models? • What new power asymmetries emerge between data holders, model aggregators, and infrastructure providers?

	• How can transparency and explainability be achieved when decision logic is distributed and adaptive? • Under what conditions does federated intelligence enhance trust and resilience?
Methodological Approaches	• Design science with blockchain-enabled federated learning and ML experimentation (Rabbani et al., 2024) • Qualitative synthesis combining expert interviews, regulatory analysis, and case studies (Slate et al., 2024) • Design science with multi-layered blockchain architecture (Javan et al., 2024) • Multiple-criteria decision analysis with evidential reasoning (Dezem et al., 2024)
Anticipated Contributions	**Theoretical:** Frameworks for distributed intelligence addressing power asymmetries, accountability gaps, and explainability challenges; a theory of trustworthy AI ecosystems requiring shared standards. **Practical:** Design patterns for blockchain-enabled federated learning, multi-layered architectures, distributed decision-support frameworks, and continuous model improvement protocols.
Value Propositions for IS Communities	**Design science research:** Prototype development and evaluation of federated learning architectures. **AI and analytics in IS:** Distributed ML/AI accountability and explainability challenges. **Socio-technical systems:** Power redistribution analysis. **Digital governance:** Governance mechanisms for distributed intelligence.

6.4 Security Collaboration as a Collective Action Problem

The panel made clear that security collaboration, the coordinated alignment of threat detection, response protocols, and risk-sharing arrangements across interdependent organisations to sustain collective resilience in shared data environments, cannot be adequately addressed through isolated organisational controls or reactive incident response in RTDSFs (Bellamkonda, 2024; Aare, 2025; Hossain et al., 2025). Security threats in real-time environments propagate across interconnected actors at speeds that often exceed contractual, regulatory, or organisational response mechanisms. While collaboration is frequently invoked as a solution, the feasibility and effectiveness of collective security arrangements remain under-theorised, particularly when participants differ significantly in size, resources, and risk exposure (Zhang et al., 2020; Javaheri et al., 2024).

For IS researchers, this reframes security collaboration as a collective action and preparedness problem rather than a technical coordination task (Table 4). Questions of liability, responsibility, and risk-sharing become central when failures originate at one node but cascade system-wide (Bellamkonda, 2024; Aare, 2025). This perspective invites research on how pre-incident coordination, shared practices, and institutional arrangements can be established under conditions where there is little time to correct errors in real-time operations (Zhang et al., 2020; Javaheri et al., 2024; Hossain et al., 2025).

Table 4. Research Agenda for Security Collaboration in RTDSFs

Theme	Description
Core Tension / Knowledge Gap	Cybersecurity research in IS has traditionally focused on organisational controls, compliance mechanisms, and post-incident response − frameworks designed for environments in which threats are largely contained within institutional boundaries and response timescales allow for deliberate action (Javaheri et al., 2024; Hossain et al., 2025). RTDSFs operate under fundamentally different conditions. Security risks propagate across interconnected actors in real time, often cascading through shared infrastructure faster than any contractual, regulatory, or organisational safeguard can respond (Zhang et al., 2020; Bellamkonda, 2024; Aare, 2025). A compromised node in a multi-stakeholder network, particularly when that node is a smaller or less mature participant, can become a vector for system-wide disruption before the breach is detected. Collaboration is frequently cited as the necessary response, yet the conditions under which effective collective security preparedness can be established remain poorly understood, especially among participants that differ substantially in size, technical maturity, regulatory exposure, and risk appetite (Javaheri et al., 2024; Bellamkonda, 2024). The core unresolved question is not whether organisations should collaborate on security, but how shared preparedness, distributed responsibility, and coordinated response can be institutionalised before incidents occur, and how the costs and liabilities of collective security are fairly distributed among structurally unequal partners (Hossain et al., 2025).
Research Questions	• How can security risks be mitigated across real-time data ecosystems? • Under what conditions does multi-stakeholder security collaboration improve real-time resilience? • How are security responsibilities and liabilities distributed when failures originate at one node but cascade across an RTDSF? • What forms of pre-incident coordination are feasible and effective in real-time environments?
Methodological Approaches	• Comparative case analysis using infrastructure metrics and regulatory reports (Bellamkonda, 2024) • Empirical analysis of production systems with architectural benchmarking (Aare, 2025) • Mixed methods combining case studies, vulnerability assessments, and interviews (Hossain et al., 2025) • PRISMA-based systematic review with topic modelling (Javaheri et al., 2024) • Design science with blockchain-based prototypes (Zhang et al., 2020)
Anticipated Contributions	**Theoretical:** Frameworks for security as networked collective action; socio-technical threat taxonomies; theories of collaborative trust via cryptographic consensus. **Practical:** Design patterns for coordinated security checkpoints, shared fraud rules and monitoring protocols, collaborative API governance, shared threat taxonomies, blockchain-mediated joint assurance.
Value Propositions for IS Communities	**Cybersecurity in IS:** Ecosystem-level threat prevention, detection, and management beyond organizational boundaries. **Inter-organizational systems:** Joint security governance and liability distribution. **Risk and resilience studies:** Cascade effects and collective resilience mechanisms. **Critical infrastructure research:**

	Pre-, during, and post-incident coordination protocols.

6.5 Interdependencies and Research Pathways

The four research pillars outlined above, Mutual Trust, Transparent Governance, Federated Intelligence, and Security Collaboration, are not independent research streams but interconnected dimensions of complex socio-technical systems. Understanding these interdependencies is essential for designing effective RTDSFs and for structuring research programs that address the whole system rather than its isolated components.

Table 5 places the four pillars side by side, articulating for each its core tension, its specific relationship to real-time conditions, and the tensions it generates in relation to the other pillars.

Table 5. Cross-Pillar Summary: Core Tensions, Real-Time Conditions, and Inter-Pillar Tensions

Pillar	Core Tension	Relationship to Real-Time Condition	Tensions with Other Pillars
1. Mutual Trust under Conditions of Speed and Automation	Existing IS trust theories assume episodic exchange and opportunities for prior validation. In RTDSFs, data must be acted upon before trust can be verified, and breakdowns may only be discovered after irreversible consequences.	Real-time automation converts trust from a deliberative relational judgment into a systemic infrastructural dependency. Validation lags action, and recovery mechanisms are rarely designed for this sequence.	Trust and governance shape each other. Governance provides the enforcement mechanisms that make trust possible at scale, yet governance frameworks themselves depend on baseline inter-organisational trust to function. Trust also conditions federated intelligence. Actors share model parameters only when they trust that aggregation layers will not be exploited.
2. Transparent Governance beyond Visibility and Disclosure	Prevailing governance models assume stable decision rights and deliberative oversight. In RTDSFs, governance must function across automated execution and cross-jurisdictional participation where oversight structurally follows rather than precedes action.	Real-time execution compresses the window for governance intervention. Rules designed for episodic compliance cannot keep pace with continuous, automated data flows, creating accountability gaps that visibility alone cannot close.	Governance and transparency create security exposure. Disclosure of system architecture, access rules, or data flows to enable accountability may simultaneously reveal attack surfaces. Governance and federated intelligence are also in tension − distributing computation across actors complicates the assignment of regulatory responsibility and may make enforcement structurally difficult.

3. Federated Intelligence as a Redistribution of Control	Federated approaches are presented as reconciling real-time analytics with privacy and sovereignty. However, distributing computation reconfigures rather than eliminates control – concentrating power at model aggregation layers that are less visible and less governed than raw data flows.	In real-time RTDSFs, federated models evolve continuously and decisions may be executed automatically. No single actor retains a complete picture of how the system is behaving at any given moment, making explainability and contestability structurally difficult.	Federated intelligence complicates governance accountability. When decision logic is distributed and adaptive, it is unclear which actor is responsible for outcomes and which regulator has jurisdiction. It also reshapes security − decentralisation reduces single points of failure but introduces new vulnerabilities at aggregation and synchronisation layers that existing security frameworks do not address.
4. Security Collaboration as a Collective Action Problem	Traditional cybersecurity focuses on organisation-centric and episodic incident management processes. In RTDSFs, threats cascade across interconnected actors in real time, faster than any single organisation can respond, making pre-incident collective preparedness the only viable defence.	The speed of real-time data flow means security failures at one node can reach system-wide scale before detection. This eliminates the response window that most security frameworks assume, converting security from an organisational to an ecosystem-level challenge.	Security and transparency are in direct tension. Sharing threat intelligence, playbooks, and system vulnerabilities to build collective preparedness also exposes attack surfaces to adversaries. Security collaboration also depends on trust. Without pre-incident trust between partners of unequal size and maturity, coordination agreements remain nominal rather than operational.

Interconnections Between Pillars. Trust and governance form a foundational relationship. Trust cannot be sustained without enforceable governance mechanisms, yet governance frameworks fail to gain traction when trust among participants is absent (Dinckol et al., 2023; Fassnacht et al., 2023). In RTDSFs, this relationship intensifies because automated execution compresses the minimal space between action and oversight, leaving little room for ex-post trust repair. Similarly, federated intelligence architectures are simultaneously a technical response to trust deficits, enabling collaboration without raw data pooling, and a governance challenge, as they redistribute control in ways that may blur accountability (Rabbani et al., 2024; Slate et al., 2024). Security collaboration, in turn, depends on both trust and governance. Without shared protocols and enforceable responsibilities, collaborative security arrangements devolve into coordination failures, particularly when threats propagate faster than contractual or regulatory mechanisms can respond (Bellamkonda, 2024; Hossain et al., 2025). Federated intelligence also reshapes security. By decentralizing data and computation, it reduces single points of failure but introduces new vulnerabilities at aggregation and coordination layers (Javaheri et al., 2024). These interdependencies suggest that advances in one pillar may create new challenges in others, and that research designs must account for systemic feedback rather than treating pillars in isolation.

Tensions and Trade-offs Between Pillars. The interdependencies above also generate genuine tensions that research designs must confront rather than resolve prematurely. First, transparency and security are in structural conflict. Disclosure of system architectures and data flows that enables

governance accountability simultaneously creates exploitable attack surfaces (Rabbani et al., 2024). Second, federated intelligence complicates governance accountability. Distributing computation reduces raw data concentration but creates accountability gaps at model aggregation layers that existing regulatory frameworks were not designed to address (Dezem et al., 2024; Slate et al., 2024). Third, panellists struck a different balance between regulatory mandates and market incentives as drivers of RTDSFs adoption − a tension reflecting different assumptions about institutional capacity and organisational behaviour that IS research has not yet resolved in real-time contexts. Fourth, the pathway from competitive hoarding to collaborative openness that Inner Source models demonstrate within organisations may not transfer straightforwardly to cross-organisational RTDSFs where intellectual property and market position are structurally at stake (Fassnacht et al., 2023). These tensions constitute the research agenda's most productive and underexplored dimension.

Sequencing and Research Priorities. While all four pillars require sustained attention, certain research questions may be more foundational than others. Establishing the governance conditions under which RTDSFs can operate transparently and enforceably appears logically prior to deploying federated intelligence at scale. Without clarity on liability, data access rights, and supervisory coordination, even technically sound federated architectures risk becoming contested or abandoned (OECD, 2023; Pflucke, 2025). Similarly, trust-building mechanisms may need to be designed into governance structures from the outset rather than retrofitted once trust breakdowns occur (Dantas and Dalziell, 2005; van Panhuis et al., 2014). Security collaboration, while often treated as an operational concern, may be most effective when embedded in governance and architectural design rather than appended as a reactive layer (Zhang et al., 2020; Aare, 2025). This sequencing logic suggests a phased research approach. Early-stage work on governance frameworks and trust mechanisms can inform subsequent research on federated intelligence architectures and collaborative security protocols. However, this is not a strict linear progression. Pilot implementations of federated intelligence or security collaboration may reveal governance gaps or trust failures that require iterative refinement, reinforcing the need for adaptive research designs.

Program Coherence and Cumulative Knowledge. To support cumulative inquiry, future research should be designed with explicit attention to how findings across pillars inform one another. For instance, case studies of governance implementation (Pillar 2) can surface trust breakdowns (Pillar 1) and security coordination failures (Pillar 4), while prototypes of federated intelligence (Pillar 3) can reveal where transparency mechanisms succeed or fail (Pillar 2). Cross-pillar research designs, such as long-term studies tracking RTDSFs from governance design through deployment to security incidents, can capture these interdependencies empirically. Methodologically, this calls for multi-method programs that combine legal-institutional analysis, qualitative case studies, design science prototyping, and systematic reviews, ensuring that theoretical, empirical, and design-oriented insights are integrated. By treating the four pillars as an interdependent system, the IS community can build a research program that combines analytical rigour with practical actionability, guiding the design of RTDSFs that are trusted, transparent, intelligent, and secure.

6.6 Reflections on the Path Forward

To finalize the research agenda, we return to the panel's participants, whose reflections capture both the challenges and the promise of RTDSFs. Their perspectives underscore that the path forward requires rigorous research alongside sustained institutional commitment and cross-sector collaboration. Technical capabilities alone cannot resolve the trust, governance, and coordination challenges inherent in real-time data sharing. The key reflections from each panellist are summarised below.

Ashish Gupta emphasized justification tied to concrete use cases. Real-time data sharing holds significant value for developing next-generation AI models in time-sensitive situations requiring low-latency decisions (capital markets, high-frequency trading, real-time streaming). However, implementation costs and infrastructure demands remain significant barriers. The justification for real-time data sharing must be directly tied to the need for real-time analytics or AI-driven use cases. Otherwise, we may simply be sharing data without deriving value (cf. Jackson, 2014). Critical parallel issues around data ownership, security, transparency, privacy, regulation, and policy must be addressed before effective implementation.

Heiko Gewald offered measured optimism grounded in technological trajectory. While recognizing today's high costs, he remains confident that over the next one or two decades, computing power will become both significantly greater and more affordable, diminishing technical barriers to real-time sharing. Healthcare is still at the beginning of this journey but heading in the right direction.

Jonna Järveläinen stressed the primacy of proactive trust-building. In high-stakes environments like energy or mining, hope must be matched by action. Real-time data sharing depends on trust built before incidents occur. SMEs often lag in cybersecurity, creating weak links in complex ecosystems. Without shared preparedness, joint protocols, exercises, and ongoing cooperation, these networks remain fragile. Collaboration across unequal partners is essential, not optional.

Lorraine Morgan highlighted organizational readiness. Real-time data sharing frameworks depend as much on inner source transformation as on external regulation. Organizations must learn to share within before they can share across. Firms that have adopted inner source demonstrate that transparency, contribution, and reuse can work at scale, preparing them to engage more effectively in federated and cross-sector ecosystems. Readiness for real-time data sharing is a matter of cultural change as much as technical infrastructure.

Stephen McCarthy positioned RTDSFs as a fundamentally socio-technical research domain, where the central challenges are organisational and political alongside the technical ones. We need to examine how these systems are built and deployed, and, just as importantly, how they shape and are shaped by organisational structures, power dynamics, and human decision-making. With the rise of agentic AI and autonomous systems, these questions become even more pressing. As technologies evolve, so too must our frameworks for accountability, governance, and trust.

These reflections collectively reinforce the research agenda's central argument − RTDSFs function as socio-technical systems. This requires alignment across technological capability, institutional governance, stakeholder trust, and organisational culture. Technical infrastructure alone cannot deliver this alignment. The path forward, as the panellists make clear, is neither simple nor guaranteed, but it is necessary, and the IS research community is uniquely positioned to guide it.

7 Conclusion

This panel report examined real-time data sharing frameworks as emerging socio-technical infrastructures that extend well beyond questions of technical feasibility into contested territory involving governance, trust, power, and collective action. The high level of engagement throughout the session, from opening polls through reflective closing commentary, underscored both the timeliness of the topic and the scale of the open questions that remain unresolved for the IS community.

Three orientations emerged from the panel discussion that this report proposes as productive anchors for future IS research. First, trust in RTDSFs calls for reframing. It operates less as a stable relational precondition and more as a systemic dependency embedded in architectures, protocols, and automated decision routines. When data must be acted upon before it can be validated, and when breakdowns may only become visible after irreversible consequences, existing IS trust theories require extension. Research into trust under conditions of speed, automation, and cross-organisational asymmetry is not yet well developed.

Second, governance emerges as the most structurally significant challenge, a direction suggested by the panel discussion and indicated, though not confirmed, by closing poll responses in which a substantial majority of participants identified enforceable governance and regulatory engagement as the most critical factors for sustainable real-time data sharing. The open research question is not whether governance matters, but how governance can be designed to be enforceable and accountable when oversight structurally follows automated execution rather than preceding it. This requires theoretical, empirical, and design-oriented inquiry that existing frameworks only partially address.

Third, the panel surfaced productive tensions that a convergence-focused synthesis would obscure. Panellists placed different weight on regulation versus market-driven incentives as the primary lever for adoption, left open how accountability should be assigned as control is redistributed across federated architectures, and raised the trade-off between pursuing transparency and avoiding new security exposure without resolving it. These tensions are offered as productive sites of disagreement that future IS research should investigate rather than prematurely settle.

The research agenda developed in Section 6 organises these open questions across four interdependent pillars − mutual trust, transparent governance, federated intelligence, and security collaboration − each sharpened to what is specifically unresolved in real-time, automated, and cross-organisational contexts. Table 5 maps the tensions between these pillars, making visible the trade-offs that any research programme in this domain must navigate.

As one panellist observed, real-time data sharing may still be at the crawling stage but movement has begun. The IS research community is well positioned to ensure that as these frameworks mature from experimental pilots into critical infrastructures, the questions of who holds power, who bears risk, and who governs are addressed with the rigour, nuance, and cross-disciplinary reach that the phenomenon demands.

Declaration of AI

The first author used Otter.ai to transcribe the recording of the panel.

References

Aare, C. R. (2025). Data risk intelligence architecture: Real-time threat detection across billions of financial transactions. *World Journal of Advanced Engineering Technology and Sciences, 15*, 919–926.

Barrett, S. and Konsynski, B. (1982). Inter-organization information sharing systems. *MIS Quarterly, 6(special)*, 93-105.

Bellamkonda, S. (2024). Securing real-time payment systems: Challenges and solutions for network security in banking. *International Journal for Multidisciplinary Research, 6*, 1–13.

Bostrom, R.P. and Heinen, J.S. (1977). MIS Problems and Failures: A Socio-Technical Perspective: Part II: The Application of Socio-Technical Theory. *MIS Quarterly, 1(4),* 11–28.

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3(2),* 77-101.

Carlile, P. R. (2002). A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development. *Organization Science, 13(4),* 442–455.

Carlile, P.R., (2004). Transferring, translating, and transforming: An integrative framework for managing knowledge across boundaries. *Organization science*, *15(5),* 555-568.

Clemons, E. K., Dewan, R. M., Kauffman, R. J., and Weber, T. A. (2017). Understanding the Information-Based Transformation of Strategy and Society. *Journal of Management Information Systems, 34(2),* 425–456.

Dantas, A., and Dalziell, E. (2005). Opportunities, barriers and challenges for implementing electronic data and information sharing frameworks in organizational response to natural disasters. *Resilient Organisations Research Programme, Department of Civil Engineering, University of Canterbury*. Retrieved from https://ir.canterbury.ac.nz/handle/10092/4389

Dezem, V., Sachan, S., Macedo, M., and Andrade Longaray, A. (2024). Optimal data-driven strategy for in-house and outsourced technological innovations by open banking APIs. *Future Business Journal, 10(1).* 116.

Dinckol, D., Ozcan, P., and Zachariadis, M. (2023). Regulatory standards and consequences for industry architecture: The case of UK open banking. *Research Policy, 52*, 104760.

Fassnacht, M., Benz, C., Heinz, D., Leimstoll, J., and Satzger, G. (2023). Barriers to data sharing among private sector organizations. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. Retrieved from https://hdl.handle.net

Grassi, L., and Lanfranchi, D. (2022). RegTech in public and private sectors: The nexus between data, technology and regulation. *Journal of Industrial and Business Economics, 49*, 441–479.

He, Y., Huang, N., Wang, L., and Sun, Y. (2025). Real-Time Sales Data, Streamer Improvisation, and Sales Performance: Evidence From Live Stream Selling. *MIS Quarterly, 49(4),* 1567-1594.

Hossain, M. A., Raza, M. A., and Rahman, J. Y. (2025). Investigating the cybersecurity implications of open banking and application programming interfaces (APIs) in the financial sector. *MINISTAL, 4*, 39–56.

Jackson, B. A. (2014). *How do we know what information sharing is really worth? Exploring methodologies to measure the value of information sharing and fusion efforts*. RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/j.ctt1287mgd

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., and Hur, J. (2024). Cybersecurity threats in fintech: A systematic review. *Expert Systems with Applications, 241*, 122697.

Javan, R., Mohammadi, M., Beheshti-Atashgah, M., and Aref, M. R. (2024). A scalable multi-layered blockchain architecture for enhanced EHR sharing and drug supply chain management. *arXiv preprint*. Retrieved from https://arxiv.org/abs/2402.17342

Kassem, J. A., De Laat, C., Taal, A., and Grosso, P. (2020). The EPI framework: A dynamic data sharing framework for healthcare use cases. *IEEE Access, 8*, 179909–179920.

Knoppers, B. M. (2014). Framework for responsible sharing of genomic and health-related data. *HUGO Journal, 8(1),* 3.

Koskinen, J. and Kimppa, K.K. (2016). An Unclear Question: Who Owns Patient Information? A Kantian Take on the Concept of Datenherrschaft. *In IFIP International Conference on Human Choice and Computers*, 3-13.

Lovestone, S., and EMIF Consortium. (2020). The European medical information framework: A novel ecosystem for sharing healthcare data across Europe. *Learning Health Systems, 4(1),* e10214.

Markus, M.L. and Rowe, F. (2023). The digital transformation conundrum: Labels, definitions, phenomena, and theories. *Journal of the Association for Information Systems*, *24*(2), 328-335.

McCarthy, S., O'Raghallaigh, P., Kelleher, C., and Adam, F. (2025). A socio-cognitive perspective of knowledge integration in digital innovation networks. *The Journal of Strategic Information Systems, 34(1),* 101871.

Modi, N. D., Kichenadasse, G., Hoffmann, T. C., Haseloff, M., Logan, J. M., Veroniki, A. A., Venchiarutti, R. L., Smit, A. K., Tuffaha, H., Jayasekara, H., Manning-Bennet, A., Morton, E., McKinnon, R. A., Rowland, A., Sorich, M. J., and Hopkins, A. M. (2023). A 10-year update to the principles for clinical trial data sharing by pharmaceutical companies: Perspectives based on a decade of literature and policies. *BMC Medicine, 21*.

Opriel, S., Möller, F., Strobel, G., and Otto, B. (2025). Data Sovereignty in Inter-organizational Information Systems: S. *Business and Information Systems Engineering, 67(6),* 833-853.

Organisation for Economic Co-operation and Development (OECD). (2023). *Open finance policy considerations*(*OECD Business and Finance Policy Papers*). Retrieved from https://doi.org/10.1787/19ef3608-en

Pflucke, F. (2025). Data access and automated decision-making in European financial law. *European Journal of Risk Regulation, 16*, 11–23.

Rabbani, H., Shahid, M. F., Khanzada, T. J. S., Siddiqui, S., Jamjoom, M. M., Ashari, R. B., Ullah, Z., Mukati, M. U., and Nooruddin, M. (2024). Enhancing security in financial transactions: A novel blockchain-based federated learning framework for detecting counterfeit data in fintech. *PeerJ Computer Science, 10*, e2280.

Reimers, K., Johnston, R. B., and Klein, S. (2014). An Empirical Evaluation of Existing is Change Theories for the Case of IOIS Evolution. *European Journal of Information Systems, 23(4),* 373–399.

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. (2019). The sociotechnical axis of cohesion for the is discipline: its historical legacy and its continued Relevance1. *MIS Quarterly, 43(3),* 695-719.

Slate, D., Parisot, A., Min, L., Panciatici, P., and Van Hentenryck, P. (2024). Adoption of artificial intelligence by electric utilities. *SSRN*. Retrieved from https://ssrn.com/abstract=4847872

Stahl, B.C. (2021). *Artificial intelligence for a better future: an ecosystem perspective on the ethics of AI and emerging digital technologies*. Springer Nature.

Trist, E.L. (1981). *The evolution of socio-technical systems (Vol. 2).* Toronto: Ontario Quality of Working Life Centre.

Van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., Heymann, D., and Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health, 14*, 1144.

Wessel, L., Peters, C., and Niederman, F. (2021). Using "Panel Reports" to Advance Scholarly Discourse: A Change in Editorial Policy and Guidelines for Panel Report Authors.*Communications of the Association for Information Systems, 49*, 379–388.

Yoo, Y., Henfridsson, O., Kallinikos, J., Gregory, R., Burtch, G., Chatterjee, S., and Sarker, S. (2024). The next frontiers of digital innovation research. *Information Systems Research, 35(4),* 1507-1523.

Zachariadis, M. (2020). Data-sharing frameworks in financial services: Discussing open banking regulation for Canada. *SSRN*. Retrieved from https://ssrn.com/abstract=2983066

Zhang, C., Gupta, A., Qin, X., and Zhou, Y. (2023). A computational approach for real-time detection of fake news. *Expert Systems with Applications, 221*, 11965.

Zhang, J., Zhong, S., Wang, T., Chao, H., Wang, J. (2020). Blockchain-based Systems and Applications: A Survey. *Journal of Internet Technology, 21(1),* 1-14.

About the Authors

Ashish Gupta is Globe Life Professor of Analytics at Raymond J. Harbert College of Business at Auburn University. His research interests are in the areas of data analytics, healthcare informatics, sports analytics, and organizational and individual performance. His recent articles have appeared in journals such as European Journal of Information Systems, Decision Sciences Journal, European Journal of Operations Research, MIT Sloan Management Review, Risk Analysis, Journal of American Medical Informatics Association, Journal of Biomedical Informatics, IEEE Transactions, Information Systems Journal, Decision Support Systems, Information Systems Frontiers, Communications of the Association for Information Systems, etc. He has published 5 edited books. Professor Gupta's research has been supported by various grant agencies and several private organizations. He has a PhD in MSIS from Spears School of Business at Oklahoma State University.

Heiko Gewald is a Research Professor of Information Management and Director of the Institute for Digital Innovation at Neu-Ulm University of Applied Sciences, Germany. His research focuses on digital innovation and digital transformation, with applications in financial services and healthcare. He has investigated the risks of over-reliance on centralized data-sharing systems and their cybersecurity implications, making significant contributions to regulatory frameworks and compliance models. His expertise in emerging data-sharing technologies, privacy-preserving mechanisms, and cybersecurity solutions aligns directly with the panel's themes of transparency and innovation in real-time data sharing.

Jonna Järveläinen is an Associate Professor at the University of Jyväskylä, Finland. Her research expertise lies in organizational cybersecurity, business continuity and responsible digital transformation in digital ecosystems. She has studied the human and organizational factors influencing cybersecurity management focusing on critical infrastructures and small and medium-sized enterprises, especially in interorganizational contexts. She employs qualitative methods and design science research. She has published in leading IS journals such as Journal of the Association for Information Systems, Communications of the Association for Information Systems, International Journal of Information Management as well as central AIS conferences. She is also actively involved in editorial work of IS journals and conferences.

Lorraine Morgan is a Professor in Digital Responsibility and Head of the Business Information Systems Discipline at the University of Galway, Ireland. She specialises in open innovation, open business models, and platform-based ecosystems, focusing on data-sharing governance and the role of transparency in digital markets. As a Principal Investigator at Lero, the Irish Software Innovation Centre, she explores Inner Source software development and decentralized data-sharing frameworks. Her research has shaped best practices for regulatory harmonization, industry collaboration, and open finance models, aligning closely with discussions on the future of Open Banking and AI-driven financial ecosystems. She has also led initiatives examining the risks of real-time data exchange in cross-sector industries.

Stephen McCarthy is a Senior Lecturer in Information Systems at University College Cork (UCC), Ireland. His research investigates digital ethics, data governance, and the unintended consequences of digital transformation. Stephen has published articles in leading peer-reviewed journals such as Information Systems Journal, The Journal of Strategic Information Systems, Internet Research, Information Systems Frontiers, Information Technology and People, and Computers in Human Behaviour. He serves as an Associate Editor for major IS journals such as CAIS and actively contributes to conference tracks on data ethics and on adaptive governance. Stephen is a distinguished member of the AIS.

Copyright © 2026 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from publications@aisnet.org.