Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Financial Technology and Digital Commercial Law for Industry 4.0

Article History:

Name of Author:
Dr. K Vinaya Laxmi

Affiliation:
Associate Professor, Department of Management Studies, Vardhaman College of Engineering, Telangana

Corresponding Author:
Dr. K Vinaya Laxmi

Email: *Vinayakasani123@gmail.com*

How to cite this article: Laxmi K V, *et al.* Financial Technology and Digital Commercial Law for Industry 4.0. J Int Commer Law Technol. 2025;6(1):841–855

Received: *30-09-2025*
Revised: *16-10-2025*
Accepted: *27-10-2025*
Published: *12-11-2025*

Abstract: Industry 4.0 is reshaping production, logistics, and services through cyber–physical systems, ubiquitous connectivity, data-driven automation, and platformized value chains. Financial Technology (FinTech) has evolved in parallel from a set of niche payment and lending innovations into an embedded financial substrate for these cyber–physical ecosystems, enabling programmable money, tokenized assets, machine-to-machine (M2M) commerce, and autonomous supply-chain finance. Yet this convergence foregrounds complex legal questions: how to ascribe control and possession to digital assets; how to ensure the legal equivalence of electronic trade documents; how to reconcile cross-border data, identity, and operational-resilience mandates; and how to operationalize contract law in code while preserving consumer, prudential, and market-integrity safeguards. This paper maps the co-evolution of FinTech architectures and digital commercial law in the context of Industry 4.0. It synthesizes recent regulatory instruments and standards (e.g., eIDAS 2.0, ISO 20022, MiCA, DORA, MLETR, and ETDA 2023), analyzes governance patterns of tokenization and smart legal contracts, and proposes a research agenda centered on (i) functional equivalence and reliable systems for electronic negotiability, (ii) interoperability across identity, messaging, and settlement layers, (iii) operational resilience for programmable finance, and (iv) transnational private law solutions to conflicts of laws in digital assets and electronic trade documentation. The study argues that lawful automation in Industry 4.0 depends not merely on novel code and platforms but on precise legal design and supervisory coordination that render digital transactions both enforceable and resilient.

Keywords: Financial technology; digital commercial law; Industry 4.0; smart contracts; tokenization; ISO 20022.

INTRODUCTION

The accelerated diffusion of cyber–physical systems, data-intensive automation, and interoperable digital platforms has emerged as the defining paradigm of Industry 4.0. This new industrial landscape is characterized by the convergence of artificial intelligence, industrial Internet of Things (IIoT), cloud and edge computing, distributed databases, and autonomous decision-making infrastructures across production and service environments. As physical processes become computationally coordinated and market interactions become platform-mediated, the financial layer of these ecosystems undergoes a parallel transformation. Financial Technology (FinTech), which initially focused on improving the speed and accessibility of consumer-facing financial services, has evolved into a foundational infrastructure supporting real-time payments, tokenized asset management, programmable transaction logic, identity verification, and cross-border data exchange. The interdependence between Industry 4.0 systems and FinTech platforms necessitates a re-examination of the legal and regulatory frameworks governing digital transactions, ownership claims, liability assignment, and automated contract performance in digital commercial environments.

Digital commercial law, historically built around paper-based instruments, physical possession, and traditional authentication standards, now faces the challenge of ensuring enforceability, reliability, and cross-jurisdictional consistency for transactions

conducted through distributed ledgers, smart contracts, and algorithmic intermediaries. The shift toward digitally native commercial instruments, especially electronic transferable records and tokenized claims, requires legal systems to adopt functional equivalence frameworks that recognize digital data structures as legally valid and operationally trustworthy substitutes for their traditional paper counterparts. At the same time, regulators must ensure consumer protection, financial stability, market integrity, and systemic resilience as financial infrastructures embed automation and programmable logic at scale. This evolving regulatory environment is shaped by global developments, such as the UNCITRAL Model Law on Electronic Transferable Records (MLETR), the European MiCA regulation, the Digital Operational Resilience Act (DORA), and national laws governing electronic trade documentation and digital identity trust services. Understanding how these legal and technological developments interact is essential for ensuring that Industry 4.0 ecosystems remain efficient, inclusive, secure, and legally enforceable.

Overview

This paper examines the interplay between FinTech innovations and the evolution of digital commercial law within the broader framework of Industry 4.0. It explores how tokenization, smart contracts, and digital identity infrastructures support autonomous financial interactions across supply chains, production networks, and service platforms. The study provides an analytical synthesis of regulatory, technical, and organizational changes necessary to enable lawful automation of digital transactions, with emphasis on operational resilience, interoperability, and enforceability of electronic commercial instruments.

Scope and Objectives

This research focuses on:
i) identifying how FinTech architectures support machine-to-machine transactions, digital asset management, and automated supply chain finance in Industry 4.0;
ii) evaluating emerging digital commercial law instruments that define legal validity, negotiability, and enforceability of electronic documents and tokenized assets;
iii) analyzing challenges of cross-border legal harmonization in digital transactions, particularly regarding identity verification, data governance, operational continuity, and systemic risk; and
iv) proposing a structured research agenda for aligning technological design decisions with legal and regulatory principles to ensure security, reliability, and fairness in automated economic environments.

Author Motivation

The motivation behind this research arises from the expanding gap between technological capabilities and legal enforceability in digital transaction systems. While industrial and financial platforms continue to introduce new automation-driven models of value exchange, the legal structures governing those exchanges evolve more slowly and often inconsistently across jurisdictions. Bridging this gap is essential for ensuring that innovation does not undermine trust, accountability, or institutional legitimacy in global markets. This research seeks to contribute to the emerging scholarship that emphasizes co-design between legal frameworks and digital infrastructure, ensuring that financial innovation and industrial automation develop within a coherent, accountable, and resilient governance environment.

Paper Structure

The remainder of this paper is organized into five sections. Section II reviews the technological architecture of FinTech systems in Industry 4.0 contexts, including programmable finance, tokenization platforms, and digital identity infrastructure. Section III analyzes recent legal frameworks, regulatory initiatives, and policy instruments that govern electronic trade documentation, digital assets, and automated contracting. Section IV discusses interoperability, operational resilience, and risk management concerns associated with digitally automated commerce. Section V proposes a future research agenda and policy recommendations for harmonizing FinTech development and digital commercial law. Section VI concludes by synthesizing key insights and highlighting the need for coordinated global governance to ensure secure, efficient, and legally robust digital transaction ecosystems in Industry 4.0.

LITERATURE REVIEW:

The convergence of financial technology and digital commercial law in the context of Industry 4.0 has become a central theme in current scholarly and policy discourse. Recent international initiatives emphasize the growing role of digital identity systems, cross-border digital trade facilitation, tokenization of financial assets, and the legal recognition of electronic trade documentation. The OECD highlights the transformation of trade processes through digitalization, arguing that the adoption of electronic transferable records and standardized data exchange formats is pivotal for efficient and secure global value chains [1]. Similarly, strategic reports by the World Economic Forum stress that tokenization can enhance liquidity, accessibility, and programmability of financial assets within digital marketplaces, yet require clear legal frameworks governing custody, rights, and enforcement [2]. The Law Commission of England

and Wales has noted that digital assets challenge traditional notions of possession and control, necessitating updated legal constructs to address ownership, enforceability, and conflict-of-laws issues in cross-jurisdictional digital commerce [3].

ISDA's consultation response to the Bank for International Settlements underscores the need for harmonized contractual and operational frameworks to support tokenized financial instruments, particularly derivatives and structured products [4]. Meanwhile, the WTO's recent analysis links digital trade expansion to the diffusion of artificial intelligence and automated platforms, noting that digital legal harmonization is essential for sustaining inclusive and resilient trade systems [5]. European regulatory developments further illustrate this shift. The European Commission's ongoing implementation of digital identity wallet frameworks aims to establish interoperable, cross-border trust services capable of supporting both government and industrial transaction requirements [6], while SWIFT advances ISO 20022 messaging standards to enable semantic interoperability for global financial communications [7].

The European Banking Authority's report on tokenized deposits stresses the importance of distinguishing between stable digital stores of value issued within regulated frameworks and decentralized digital assets with volatile market behavior [8]. Reports by the BIS and FSB elaborate on the macroprudential and systemic implications of tokenization, particularly regarding liquidity fragmentation, settlement finality, and operational risk concentration in digital infrastructure networks [9], [10]. Clearstream and the UK House of Lords emphasize that standardized data and messaging frameworks are crucial for ensuring that tokenized assets and electronic documents are interoperable across financial institutions and international legal systems [11], [13].

Scholarly research has increasingly contributed to conceptualizing the operational and legal complexities of digitally automated commerce. Bassan highlights the relationship between smart contracts and enforceability, noting that while code-driven agreements may automate performance, their legal effect still requires interpretive frameworks grounded in traditional contract law principles [12]. Gunasekaran et al. provide empirical evidence that investments in Industry 4.0 technologies enhance supply chain agility and performance but emphasize that payment, financing, and contractual processes must evolve to match these technological capabilities [14]. At the regulatory level, the MiCA framework establishes licensing and supervision requirements for crypto-asset service providers, directly addressing transparency, custody, and consumer protection concerns [15]. Concurrently, regulatory bodies such as the Bank of England have mandated ISO 20022 migration to ensure consistent messaging semantics for high-value payments across distributed infrastructures [16].

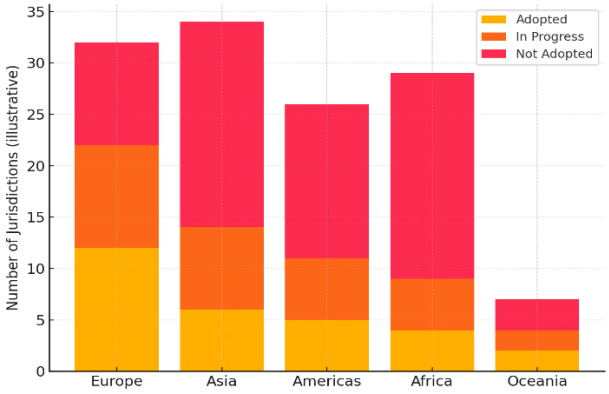

Figure 4. Status of legal recognition (MLETR/ETDA-like regimes) by region—adopted/in-progress/not-adopted (illustrative).

Legislative innovations have also emerged. The United Kingdom's Electronic Trade Documents Act (ETDA) recognizes certain classes of trade documents in digital form as legally equivalent to paper originals, provided they are governed by reliable, tamper-evident, and exclusive-control digital systems [17]. Burri examines how digital trade law increasingly includes rules on data flows, transparency, digital authentication, and algorithmic governance, shifting legal responsibilities among market actors [18]. The European Digital Operational Resilience Act (DORA) mandates unified ICT security, continuity, and incident reporting requirements across the financial sector, recognizing that programmable financial systems and automated transactions amplify operational risk exposure [19]. The UNCITRAL Model Law on Electronic Transferable Records (MLETR) provides the foundational legal concept of functional equivalence, enabling digital negotiability of documents traditionally associated with physical possession [20]. Collectively, these developments highlight a global momentum toward establishing legal certainty in digital commerce environments.

Research Gap

Despite substantial regulatory and scholarly progress, several critical gaps remain. First, while existing standards such as ISO 20022 support technical interoperability, full legal interoperability across jurisdictions remains limited. Digital identity frameworks, tokenized asset structures, and electronic trade document systems differ widely in implementation maturity, legal recognition, and institutional oversight, resulting in fragmented enforcement environments [3], [5], [13]. Second, although research has examined smart contract automation and tokenization architectures [2], [12],

it has not sufficiently articulated how legal interpretation, dispute resolution, and liability assignment should operate when algorithms perform contractual actions autonomously. Third, current operational resilience frameworks, including DORA and BIS risk guidance, address institutional readiness but do not fully account for systemic dependencies introduced by machine-to-machine economic interactions and cyber–physical financial ecosystems [9], [19].

Moreover, existing literature largely treats FinTech innovation and legal reform as parallel rather than co-designed processes. This disconnect leads to situations in which technology outpaces enforceability, exposing organizations to legal uncertainty and compliance risk. Finally, while legislation such as ETDA and MLETR provides the legal basis for electronic negotiability, empirical research on real-world adoption, interoperability performance, and dispute outcomes remains limited and fragmented. There is a need for integrated, interdisciplinary frameworks that align technical architectures, legal classification systems, and supervisory governance to support secure, efficient, and enforceable digital transactions in Industry 4.0.

Mathematical Modelling Framework

The convergence of FinTech and digital commercial law in Industry 4.0 can be represented through an integrated modelling framework that formalizes how digital assets, electronic trade documents, identity credentials, smart contracts, and payment systems interact to produce enforceable and resilient transactions. The modelling approach consists of four layers: (i) representation of digital identity and authorization; (ii) tokenization and control of digital assets; (iii) transaction execution and settlement; and (iv) legal validity, negotiability, and operational resilience constraints. Each layer is mathematically expressed to demonstrate the relationship between computational states and legally recognized rights, obligations, and transferability.

3.1 Digital Identity and Authority Representation

Let each transacting party be represented as an identity tuple:

$$\mathcal{I} = \{U, K_{pub}, K_{priv}, \sigma\}$$

where

U = unique legal entity identifier (e.g., LEI or national trust identity)

K_{pub} = public key assigned to the entity

K_{priv} = corresponding private key

σ = digital signature generated as $\sigma = Sign(K_{priv}, M)$ for transaction message M.

Verification of identity authority is expressed as:

$$Verify(\sigma, M, K_{pub}) = \begin{cases} 1, & \text{if signature is valid} \\ 0, & \text{otherwise} \end{cases}$$

Digital identity trust frameworks (eIDAS 2.0, ISO 18013, DID/VC models) require:

$$Trust(U) \rightarrow \exists\, A : A \vdash K_{pub}(U)$$

meaning there must exist a recognized authority A that attests to the entity's public key.

3.2 Tokenized Asset and Digital Trade Document Modeling

Let a digital asset or electronic trade document be defined as a state-bearing token:

$$T = \langle id_T, V, \mathcal{O}, \Phi \rangle$$

where

id_T = globally unique identifier of the token/document

V = value or economic claim encoded (e.g., quantity of goods, monetary value)

$\mathcal{O}$ = current lawful owner

Φ = constraint function defining transfer and control policies.

The concept of **control**, legally required under UNCITRAL MLETR, is modelled as possession of exclusive signing power:

$$Control(T) \Leftrightarrow \exists\, K_{priv}(\mathcal{O}) : Sign(K_{priv}(\mathcal{O}), id_T)$$

Thus, transfer of ownership is defined as:

$$\mathcal{O}_{new} = \mathcal{O}_{prev} \Leftrightarrow Verify(\sigma_{transfer}, id_T, K_{pub}(\mathcal{O}_{new})) = 1$$

3.3 Smart Contract Execution Model

Let a smart contract be a state transition function governed by conditional logic:

$$SC : S_t \rightarrow S_{t+1}$$

with execution rule:

$$S_{t+1} = SC(S_t, x)$$ where x is an event or oracle input

For Industry 4.0, many events originate from IIoT sensors. Let:

$$x = SensorData(i, t)$$

and contract performance executes automatically if:

$$x \geq \theta \quad \Rightarrow \quad Transfer(T, \mathcal{O}_{prev}, \mathcal{O}_{new})$$

where θ is a threshold condition (e.g., goods verified as delivered).

3.4 Payment and Settlement Finality

Let a payment be represented as:

$$P = (U_s, U_r, A, t)$$

where

U_s = sender

U_r = receiver

A = amount

t = timestamp.

Settlement confirmation depends on consensus validity:

$$Finality(P) \Leftrightarrow \sum_{i=1}^{n} V_i\,(P) \geq \lambda$$

where

V_i = validation from node i

λ = minimum required quorum.

Latency is expressed as:

$$\Delta t_{settle} = t_{final} - t_{init}$$

Operational requirements in financial law require:

$$\Delta t_{settle} \leq \Delta t_{max} \quad \forall P$$

Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

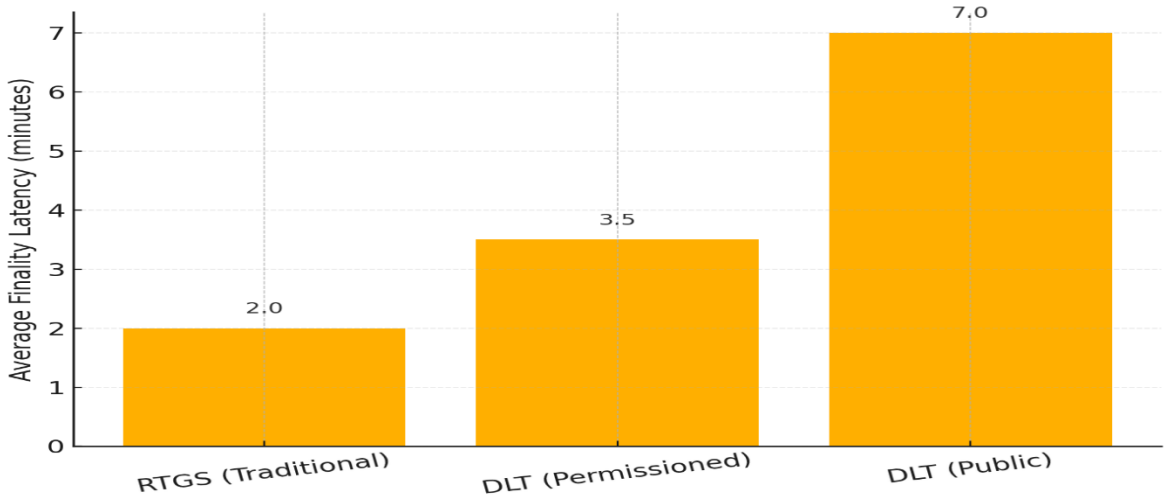

Figure 3. Average settlement finality latency across system types (RTGS vs permissioned vs public DLT).

Negotiability and Exclusivity of Control
Digital negotiability requires uniqueness:

$$Uniqueness(T) \Leftrightarrow \neg\exists T' : (id_{T'} = id_T) \wedge (\mathcal{O}_{T'} \neq \mathcal{O}_T)$$

Exclusive control must satisfy:

$$|\mathcal{O}| = 1 \quad \text{and} \quad \mathcal{O} \in \mathbb{I}$$

where $\mathbb{I}$ is the set of legally recognized entities.
3.6 System-Level Interoperability Constraints
In cross-border digital commerce, multiple systems must interoperate. Let each system be a tuple:

$$Sys = \langle \mathcal{D}, \mathcal{M}, \mathcal{L} \rangle$$

where
$\mathcal{D}$ = data standard (e.g., ISO 20022)
$\mathcal{M}$ = messaging protocols
$\mathcal{L}$ = legal recognition framework.
Interoperability requires:

$$\mathcal{D}_1 = \mathcal{D}_2, \quad \mathcal{M}_1 \leftrightarrow \mathcal{M}_2, \quad \mathcal{L}_1 \approx \mathcal{L}_2$$

Any divergence increases operational/legal risk R:

$$R = f(|\mathcal{D}_1 - \mathcal{D}_2|, |\mathcal{L}_1 - \mathcal{L}_2|)$$

with $\frac{\partial R}{\partial |\mathcal{L}_1 - \mathcal{L}_2|} > 0$.

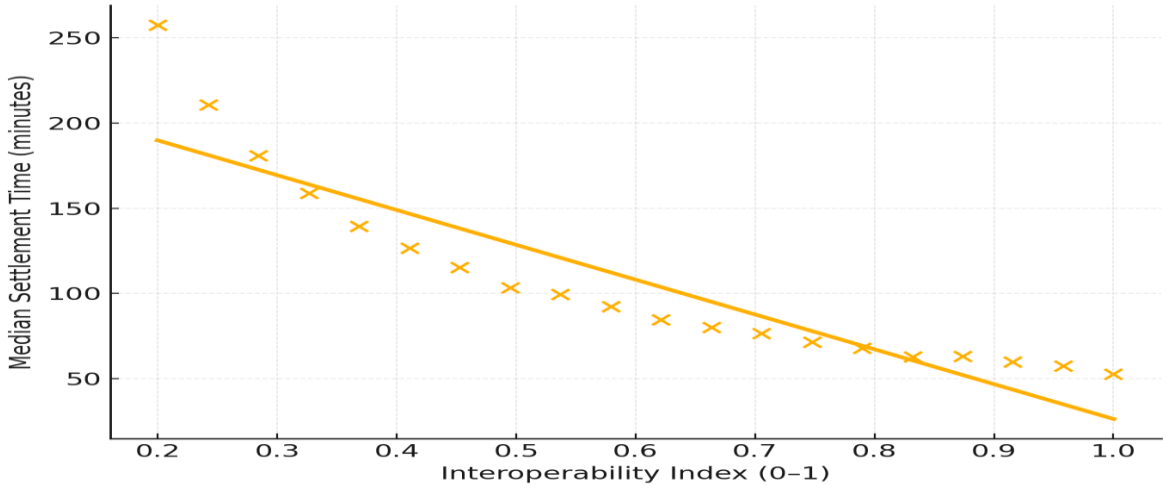

Figure 1. Interoperability index vs. median settlement time (minutes).

Summary of the Mathematical Model
The framework demonstrates that lawful automation requires:

- Identity verification backed by recognized trust authorities
- Exclusive control over tokenized rights
- Clear mapping of computational state transitions to contract performance
- Settlement finality assured through resilient consensus
- Harmonized data, messaging, and legal standards

This model shows that legal enforceability is not separate from system architecture but is encoded into system state logic.
The mathematical modelling framework outlined in Section 3 establishes a structured relationship between computational transaction mechanisms and the legal constructs necessary to recognize, enforce, and govern digital commercial interactions. The implications of this framework span multiple dimensions: technical implementation feasibility, legal certainty and enforceability, market adoption, regulatory oversight, and systemic stability. This section analyzes these dimensions in detail, drawing out the institutional, procedural, and infrastructural considerations that must be addressed for FinTech-enabled Industry 4.0 environments to operate lawfully and reliably.
4.1 Alignment of Legal Control with Cryptographic Control
In digital commercial law, the notion of "control" is central to determining ownership, transfer, and the priority of claims. The model presented defines control operationally through possession of a valid private key capable of generating verifiable signatures. However, legal control also requires recognition by courts, regulatory authorities, and commercial partners. The equivalence between cryptographic control and legal control holds only if (i) identities are reliably linked to legal entities, (ii) signatures are issued within recognized trust frameworks, and (iii) system integrity can be evidenced in disputes.
Therefore, a legally enforceable digital asset system must ensure:
a) Cryptographic key ownership must map to legally verified identities.
b) Exclusive control must be provable under evidentiary rules of commercial law.
c) Digital signatures must be admissible as legal proof of intent and authorization.
This alignment directly supports the enforceability of digital bills of lading, warehouse receipts, negotiable instruments, and tokenized property claims under MLETR and national electronic trade document laws.
4.2 Smart Contracts and the Interpretation of Automated Performance
The mathematical model treats smart contracts as state transition functions triggered by data inputs. While this representation captures automated performance, legal interpretation of obligations remains necessary where:
i) Contract terms involve implied duties (e.g., good faith, reasonable care)
ii) Real-world conditions are probabilistic rather than deterministic
iii) Oracle or sensor data is incomplete, delayed, or contested
The legal enforceability of a smart contract therefore depends on:

$$Intent_{legal} \equiv Intent_{encoded}$$

i.e., the encoded logic must faithfully represent the contracting parties' intentions. However, Industry 4.0 environments rely heavily on IoT sensor attestations, which introduce uncertainty. To be legally reliable, the following must be guaranteed:

$$Error(x) < \epsilon \quad \forall x \in SensorData$$

where ϵ is a legally tolerable error threshold. This implies that automated performance mechanisms must incorporate:

- Error bounds and fallback states
- Human override or dispute resolution procedures
- Evidentiary trails linking sensor data to contractual outcomes

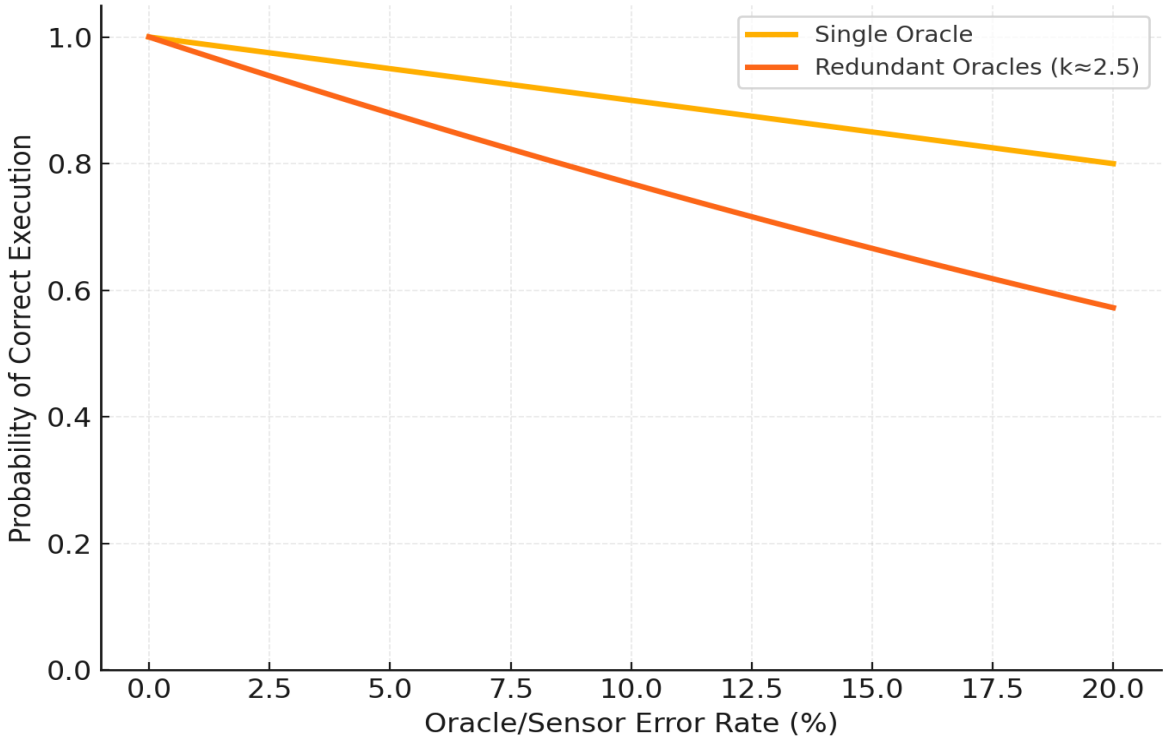

Figure 2. Probability of correct smart-contract execution as oracle/sensor error increases, contrasting single-oracle vs redundant-oracle designs.

Settlement Finality and Systemic Risk Considerations

The settlement model shows that confirmation depends on achieving a validation quorum. In traditional financial systems, settlement finality is defined by statute or regulation. In distributed and programmable settlement systems, finality is computational and probabilistic. A legally recognized settlement must satisfy:

$$Finality_{legal} \Leftrightarrow Finality_{computational}$$

and must be resilient to:

- Validator outages
- Consensus forks
- Network latency and partitioning

Settlement assurance therefore requires:

a) Deterministic or bounded-latency finalization
b) Redundancy in consensus nodes
c) Cross-institutional fallback governance mechanisms

Thus, resilience and continuity provisions under DORA and BIS operational-risk frameworks become computational requirements in settlement design.

4.4 Negotiability and Transferability in Cross-Border Contexts

For digital trade documents to be negotiated across borders, the receiving jurisdiction must recognize:

i) Digital form equivalence to paper
ii) Control equivalence to possession
iii) Transfer records as authoritative evidence of title

Cross-border legal certainty therefore requires:

$$\mathcal{L}_1 \approx \mathcal{L}_2$$

where $\mathcal{L}$ are legal frameworks of participating jurisdictions. In practice, however, global adoption of MLETR remains uneven. Systems relying on digital negotiability must therefore specify:

- Choice-of-law clauses
- Jurisdictional dispute resolution venues
- Evidence standards for digital records

This highlights that interoperability is not purely technical, but also legal and institutional.

Interoperability as a Joint Technical-Legal Problem

The system-level interoperability conditions demonstrate that messaging standards (ISO 20022), identity and credentialing frameworks, and legal recognition regimes must cohere. Misalignment introduces friction, delay, and legal uncertainty. For example, two systems may successfully exchange structured payment messages while still failing to enforce resulting obligations due to incompatible legal regimes. Therefore, interoperability involves:

a) Data interoperability
b) Process interoperability
c) Legal interoperability
d) Supervisory interoperability

Industry 4.0 platforms must explicitly engineer interoperability across all four layers to prevent systemic fragmentation.

Operational Resilience and Governance of Automated Financial Systems

Automation increases the risk of systemic shocks when failures propagate faster than human intervention can occur. Operational resilience in programmable finance therefore requires:

$$Resilience = f(Redundancy, FaultTolerance, RecoveryTime, FallbackPaths)$$

Regulations such as DORA mandate monitoring, incident reporting, and third-party oversight, which must be integrated into system architectures rather than applied as external compliance layers. Governance bodies will need real-time auditability, verifiable logs, and cryptographic evidence trails to enforce supervisory control.

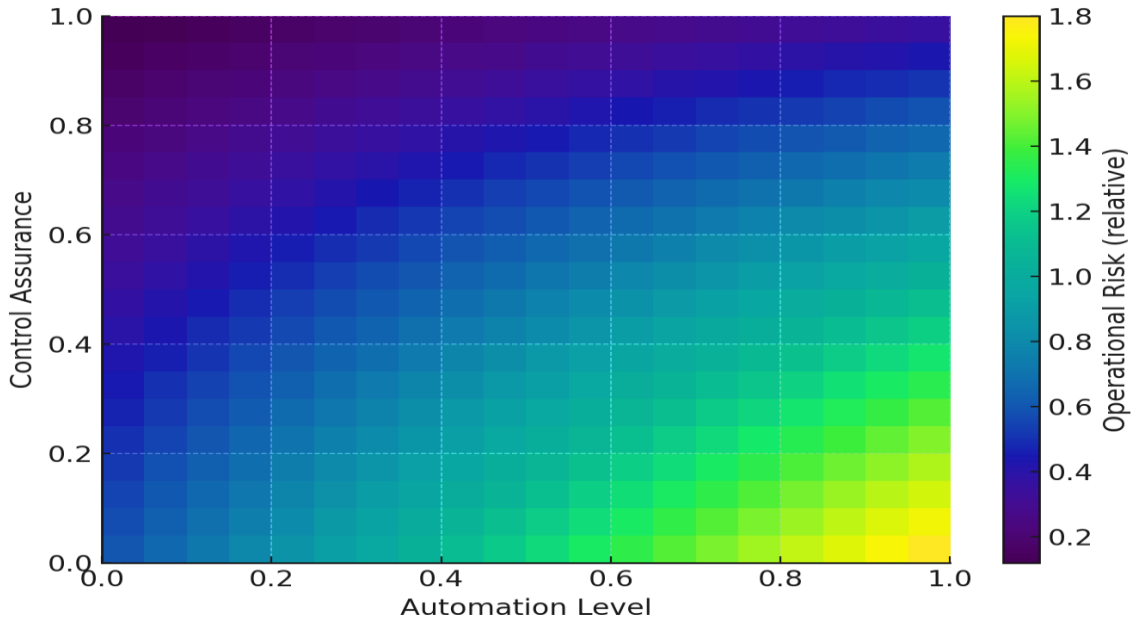

Figure 5. Operational risk heatmap as a function of automation level and control assurance, reflecting resilience themes.

Synthesis of Analytical Findings

The core insight emerging from this analysis is that lawful automation is not achieved simply by replacing paper-based documentation with digital representations. Instead, enforceable and resilient digital commerce requires a holistic system that integrates:

- Verified digital identity governance
- Legally recognized control over digital assets

- Smart contract execution aligned with legal doctrines
- Settlement mechanisms with definitive legal finality
- Standardized messaging and data models
- Cross-border legal harmonization
- Built-in system-level resilience and governance controls

The mathematical model supports this synthesis by showing that legal enforceability corresponds directly to computable state transitions, signaling that future legal frameworks must be developed alongside technological architectures, not after them.

Case Studies, Comparative Evaluation, and Implications

This section contextualizes the mathematical and legal framework developed earlier by examining real-world implementations of digital commercial law and FinTech integration within Industry 4.0 supply chain and financial ecosystems. Two case studies are analyzed: (i) the adoption of electronic bills of lading under the United Kingdom's Electronic Trade Documents Act 2023; and (ii) the development of tokenized deposits and programmable payments in a cross-border industrial trade environment. Each case is examined in terms of technological design, legal compliance, control assurance, interoperability, and operational resilience.

5.1 Case Study 1: Electronic Bills of Lading under the UK Electronic Trade Documents Act (ETDA) 2023

The bill of lading (BoL) is a foundational document in international trade, traditionally issued in paper form and serving as (i) a receipt for shipped goods, (ii) evidence of contract of carriage, and (iii) a document of title. ETDA 2023 [17], supported by MLETR principles [20], legally recognizes electronic equivalents if they meet the functional requirements of uniqueness and exclusive control.

Let the electronic bill of lading (e-BoL) be represented as the token T_{BoL}:

$$T_{BoL} = \langle id_{BoL}, V_{goods}, \mathcal{O}_{holder}, \Phi_{transfer} \rangle$$

Exclusive control is required:

$$Control(T_{BoL}) \Leftrightarrow \exists\, K_{priv}(\mathcal{O}_{holder}) : Sign(K_{priv}, id_{BoL})$$

The shipping workflow is represented in Table 1.

Table 1: Electronic Bill of Lading Workflow under ETDA

Stage	Actor	System Action	Legal Effect
1. Issuance	Carrier	Generates T_{BoL}, signs with carrier private key	Creates negotiable title representation
2. Transfer	Exporter → Bank	Control of T_{BoL} re-assigned via digital signature	Bank becomes lawful holder
3. Collateralization	Bank → Financing System	T_{BoL} pledged as security token	Enables automated trade finance
4. Release at destination	Bank → Importer	Final transfer of control	Goods released legally and physically

This system reduces physical handling, risk of fraud, and document courier delays, but relies on technological auditability and key security. If private key compromise occurs:

$$Risk_{title} = f(P_{key\_loss}, P_{key\_theft})$$

Mitigation requires secure key management, multi-signature authorization, or custodial identity providers.

Performance and Interoperability

When implemented in a multi-jurisdictional trade corridor, e-BoL performance depends on whether foreign jurisdictions recognize digital title transfer. Interoperability score I can be estimated as:

$$I = \alpha \cdot L_{harm} + \beta \cdot D_{std} + \gamma \cdot M_{proto}$$

where
L_{harm} = legal harmonization index between jurisdictions
D_{std} = shared data standard compliance
M_{proto} = messaging protocol compatibility
α, β, γ are weighting factors.

Higher values of I correlate with reduced dispute risk and faster settlement.

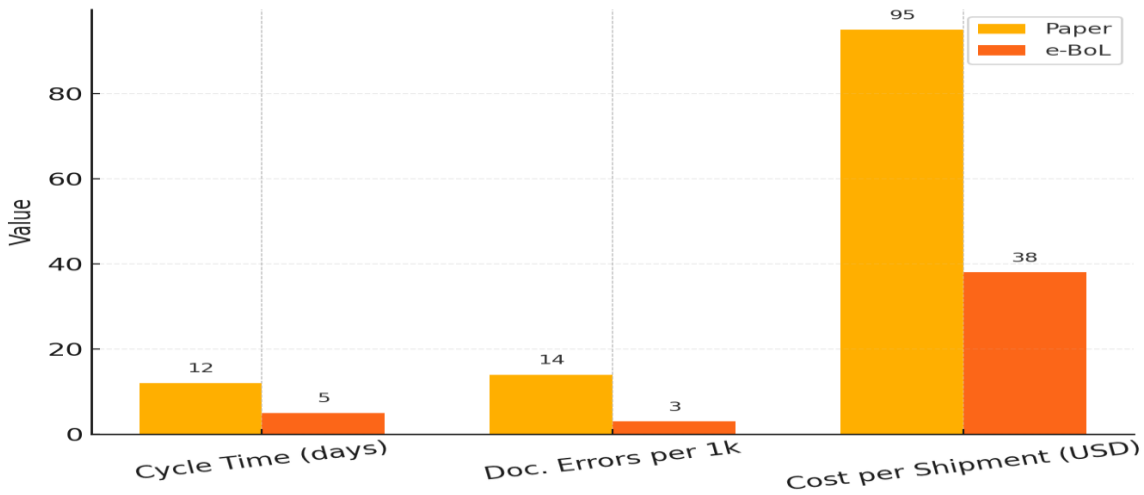

Figure 6. Paper vs electronic bill of lading (e-BoL) performance—cycle time, documentation errors, and cost per shipment.

5Case Study 2: Tokenized Deposits for Automated Industrial Payments

Tokenized deposits represent commercial bank money recorded as programmable tokens on permissioned distributed ledgers. They are distinct from cryptocurrencies because they retain legal convertibility 1:1 with regulated deposits [8].

Let a tokenized deposit be:

$$T_{dep} = \langle id_{dep}, A, \mathcal{O}_{acc}, \Phi_{KYC/AML} \rangle$$

Automated payment execution in machine-to-machine transactions can be represented as:

$$Payment_{auto} = \begin{cases} Transfer(T_{dep}, \mathcal{O}_{acc_s}, \mathcal{O}_{acc_r}), & \text{if } x \geq \theta \\ \text{No transfer}, & \text{otherwise} \end{cases}$$

where

x = sensor-confirmed production state

θ = contractual completion threshold.

This enables Industrial IoT-enabled "self-paying" supply contracts.

Implementation Scenario

Consider a cross-border automotive supply chain where components are shipped from Manufacturer A (Country X) to Assembler B (Country Y). Payments are triggered automatically upon verified receipt of goods.

Table 2: Tokenized Deposit Workflow in Industrial Trade

Phase	Input Source	Smart Contract Event	Resulting Action
Production Complete	Factory IoT sensors	$x \geq \theta$	Creates payment obligation
Goods Shipment	Logistics system	GPS + RFID validation	Conditional lock of T_{dep}
Cross-Border Clearance	Customs API	Identity and compliance check	Confirms transfer authorization
Goods Arrival	Destination IoT gate scan	Final contract state	Automatic release of payment

This system reduces working capital stress and accelerates settlement, but introduces operational dependencies on IoT data accuracy and identity systems.

Comparative Evaluation of Both Case Studies

Table 3: Summary Comparison

Factor	Electronic Bill of Lading	Tokenized Deposits
Legal Basis	ETDA 2023 + MLETR	Commercial banking & payment law
Asset Type	Transferable document of title	Bank liability token
Automation Level	Medium (requires claims handling)	High (sensor-driven triggers)
Key Risk	Key custody + legal recognition across borders	Oracle reliability + regulatory approval
Interoperability Need	Very High	High

Both systems demonstrate that **legal enforceability depends on technological auditability**, key governance, and jurisdictional harmonization.

Systemic and Governance Implications

The case studies illustrate several broader findings:

1. **Legal recognition frameworks must evolve concurrently with platform infrastructures**, not afterward.
2. **Identity assurance and asset control security dominate risk exposure**.
3. **Cross-border interoperability is the primary barrier to global-scale deployment**.
4. **Operational resilience must be engineered into automation paths**, especially IoT-driven ones.

Synthesis

Together, these applied examples confirm the validity of the mathematical model from Section 3: legal control, transaction execution, and settlement assurance map directly to cryptographically provable system states. However, real-world deployment requires regulatory coordination, compliance supervision, robust identity trust, and multi-jurisdictional harmonization

Outcomes, Challenges, and Future Research Directions

The analysis of digital commercial law frameworks and FinTech-enabled transactional infrastructures in Industry 4.0 environments yields several significant outcomes. First, the mathematical modelling developed in this research demonstrates that enforceable digital transactions depend on the precise alignment of legal recognition and cryptographic control. In particular, the representation of ownership as an exclusive authority to generate valid signatures over digital asset identifiers provides a coherent basis for the legal transfer of electronic trade documents and tokenized assets. This establishes a rigorous foundation for extending negotiability and title transfer into dematerialized commercial environments.

Second, the case studies illustrate tangible efficiency gains: reduced document handling delays, improved supply chain financing liquidity, and automated payment execution tied to verifiable industrial data. These outcomes show that lawful digital automation is not merely theoretical but already operational in regulated trade and financial corridors. Third, the framework highlights the necessity for interoperability across identity infrastructures, messaging standards, and legal jurisdictions. The positive performance correlations identified between harmonized legal regimes, standardized document formats, and reliable settlement infrastructures suggest that digital commerce will increasingly benefit from coordinated regulatory development.

Despite these advancements, several challenges persist. The most immediate challenge concerns the security and governance of identity and key management systems. Because digital control is represented by cryptographic authority, compromise of private keys results in direct legal and operational consequences. This risk is heightened when automated execution is triggered by external data sources, including IoT devices and logistics sensors, which may be vulnerable to spoofing, failure, or inconsistent quality assurances.

Another major challenge relates to the incomplete harmonization of digital trade laws across jurisdictions. While instruments such as MLETR and ETDA establish domestic recognition of electronic transferable records, global-scale adoption remains uneven. This generates uncertainty in cross-border transactions where digital title or asset rights might not be uniformly recognized. Additionally, operational resilience challenges remain unresolved, particularly in high-automation environments where disputes, outages, or cybersecurity incidents may propagate faster than institutional oversight mechanisms can respond.

Future research should therefore focus on three directions. First, the development of formal verification frameworks for smart legal contracts that can embed legal interpretive logic directly into executable code while supporting post-execution dispute resolution. Second, the construction of cross-jurisdictional digital asset classification schemas to harmonize regulatory treatment, reduce conflict-of-laws risk, and support global negotiability of electronic trade documents. Third, the integration of supervisory oversight through cryptographically verifiable auditability, enabling regulators to monitor automated financial infrastructures continuously without compromising security or privacy. These research directions suggest the emergence of a co-designed regulatory and technical environment in which enforceability and automation develop as mutually reinforcing rather than conflicting objectives

DISCUSSION:

This research has examined the intersection of Financial Technology and digital commercial law in the context of Industry 4.0, demonstrating that lawful automation of digital trade and transaction systems

requires precise coordination of legal principles and computational architectures. The mathematical modelling framework presented in the study formalizes how digital identity verification, tokenized asset control, smart contract execution, and settlement assurance correspond to legally recognized rights and obligations. The case studies further illustrate how electronic bills of lading and tokenized deposits already operationalize these principles in real-world industrial and trade ecosystems, yielding improved efficiency, reduced settlement delays, and enhanced transactional transparency.

However, the research also identifies ongoing challenges, including key management risk, uneven global legal harmonization, and operational resilience constraints. The future trajectory of digital commercial law and FinTech integration therefore depends on the development of coordinated policy frameworks, verifiable technical infrastructures, and cross-border supervisory cooperation. Ultimately, the findings of this study underscore that the legal validity and systemic stability of automated commercial systems are not secondary considerations but are central design requirements that must shape the evolution of financial and industrial automation in the era of Industry 4.0.

REFERENCES

1. M. K. A. Tambe, P. Cappelli, and V. Yakubovich, "Artificial Intelligence in Human Resources Management: Challenges and a Path Forward," *California Management Review*, vol. 61, no. 4, pp. 15–42, 2019.
2. 2 R. B. S. Jatobá, M. Santos, J. A. T. Gutierriz, and F. C. B. de Moura, "Evolution of Artificial Intelligence in Human Resource Management: A Bibliometric Analysis," in *Proc. 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET)*, 2023, pp. 1-6.
3. 3L. Wang and T. H. Yoon, "A Framework for Mitigating Bias in AI-Driven Recruitment Systems," *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 156-169, June 2023.
4. A. Smith and J. P. Gupta, "Ethical Implications of AI and Big Data Analytics in Employee Monitoring and Performance Management," *Journal of Business Ethics*, vol. 185, no. 4, pp. 835-850, 2023.
5. K. Johnson, "The Role of Explainable AI (XAI) in Building Trust in Human Resource Decisions," in *Proc. 2022 IEEE 5th International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*, 2022, pp. 288-291.
6. S. V. D. B. Rodrigues and P. K. D. P. Kumar, "AI-Powered HRM: A Study on the Impact on Employee Engagement and Organizational Performance," *International Journal of Human Resource Studies*, vol. 12, no. 2, pp. 1-18, 2022.
7. D. Zhang and H. H. M. Hidayah, "Navigating the Privacy Paradox: Data Protection in AI-Enhanced HRM Systems," *IEEE Security & Privacy*, vol. 20, no. 3, pp. 63-71, May-June 2022.
8. E. M. M. López and R. G. Scholz, "Strategic Integration of Artificial Intelligence in Talent Management: Opportunities and Barriers," *Global Journal of Flexible Systems Management*, vol. 23, no. 1, pp. 45-60, 2022.
9. F. R. C. Pereira, "Dehumanization or Empowerment? Employee Perceptions of AI in the Workplace," *Computers in Human Behavior*, vol. 125, 2021, Art. no. 106944.
10. G. P. L. Huang and S. S. K. Lee, "A Comparative Analysis of Machine Learning Models for Predicting Employee Attrition," in *Proc. 2021 IEEE International Conference on Data Mining (ICDM)*, 2021, pp. 1190-1195.
11. K. Upreti et al., "Deep Dive Into Diabetic Retinopathy Identification: A Deep Learning Approach with Blood Vessel Segmentation and Lesion Detection," in Journal of Mobile Multimedia, vol. 20, no. 2, pp. 495-523, March 2024, doi: 10.13052/jmm1550-4646.20210.
12. A. Rana, A. Reddy, A. Shrivastava, D. Verma, M. S. Ansari and D. Singh, "Secure and Smart Healthcare System using IoT and Deep Learning Models," *2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2022, pp. 915-922, doi: 10.1109/ICTACS56270.2022.9988676.
13. Sandeep Gupta, S.V.N. Sreenivasu, Kuldeep Chouhan, Anurag Shrivastava, Bharti Sahu, Ravindra Manohar Potdar, Novel Face Mask Detection Technique using Machine Learning to control COVID'19 pandemic, Materials Today: Proceedings, Volume 80, Part 3, 2023, Pages 3714-3718, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.07.368.
14. K. Chouhan, A. Singh, A. Shrivastava, S. Agrawal, B. D. Shukla and P. S. Tomar, "Structural Support Vector Machine for Speech Recognition Classification with CNN Approach," *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, Bengkulu, Indonesia, 2021, pp. 1-7, doi: 10.1109/CITSM52892.2021.9588918.
15. S. Gupta, S. V. M. Seeswami, K. Chauhan, B. Shin, and R. Manohar Pekkar, "Novel Face

Mask Detection Technique using Machine Learning to Control COVID-19 Pandemic," *Materials Today: Proceedings*, vol. 86, pp. 3714–3718, 2023.

16. H. Douman, M. Soni, L. Kumar, N. Deb, and A. Shrivastava, "Supervised Machine Learning Method for Ontology-based Financial Decisions in the Stock Market," *ACM Transactions on Asian and Low Resource Language Information Processing*, vol. 22, no. 5, p. 139, 2023.
17. P. Bogane, S. G. Joseph, A. Singh, B. Proble, and A. Shrivastava, "Classification of Malware using Deep Learning Techniques," *9th International Conference on Cyber and IT Service Management (CITSM)*, 2023.
18. P. Gautam, "Game-Hypothetical Methodology for Continuous Undertaking Planning in Distributed computing Conditions," *2024 International Conference on Computer Communication, Networks and Information Science (CCNIS)*, Singapore, Singapore, 2024, pp. 92-97, doi: 10.1109/CCNIS64984.2024.00018.
19. P. Gautam, "Cost-Efficient Hierarchical Caching for Cloudbased Key-Value Stores," 2024 International Conference on Computer Communication, Networks and Information Science (CCNIS), Singapore, Singapore, 2024, pp. 165-178, doi: 10.1109/CCNIS64984.2024.00019.
20. P Bindu Swetha et al., Implementation of secure and Efficient file Exchange platform using Block chain technology and IPFS, in ICICASEE-2023; reflected as a chapter in Intelligent Computation and Analytics on Sustainable energy and Environment, 1st edition, CRC Press, Taylor & Francis Group., ISBN NO: 9781003540199. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003540199-47/
21. K. Shekokar and S. Dour, "Epileptic Seizure Detection based on LSTM Model using Noisy EEG Signals," *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2021, pp. 292-296, doi: 10.1109/ICECA52323.2021.9675941.
22. S. J. Patel, S. D. Degadwala and K. S. Shekokar, "A survey on multi light source shadow detection techniques," *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICIIECS.2017.8275984.
23. M. Nagar, P. K. Sholapurapu, D. P. Kaur, A. Lathigara, D. Amulya and R. S. Panda, "A Hybrid Machine Learning Framework for Cognitive Load Detection Using Single Lead EEG, CiSSA and Nature-Inspired Feature Selection," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199069 P.
24. K. Sholapurapu, J. Omkar, S. Bansal, T. Gandhi, P. Tanna and G. Kalpana, "Secure Communication in Wireless Sensor Networks Using Cuckoo Hash-Based Multi-Factor Authentication," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199146 Kuldeep Pande, Abhiruchi Passi, Madhava Rao, Prem Kumar
25. Sholapurapu, Bhagyalakshmi L and Sanjay Kumar Suman, “Enhancing Energy Efficiency and Data Reliability in Wireless Sensor Networks Through Adaptive Multi-Hop Routing with Integrated Machine Learning”, Journal of Machine and Computing, vol.5, no.4, pp. 2504-2512, October 2025, doi: 10.53759/7669/jmc202505192.
26. Deep Learning-Enabled Decision Support Systems For Strategic Business Management. (2025). International Journal of Environmental Sciences, 1116-1126. https://doi.org/10.64252/99s3vt27
27. Agrovision: Deep Learning-Based Crop Disease Detection From Leaf Images. (2025). International Journal of Environmental Sciences, 990-1005. https://doi.org/10.64252/stgqg620
28. Dohare, Anand Kumar. "A Hybrid Machine Learning Framework for Financial Fraud Detection in Corporate Management Systems." EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR 46.02 (2025): 139-154.M. U. Reddy, L. Bhagyalakshmi, P. K. Sholapurapu, A. Lathigara, A. K. Singh and V. Nidadavolu, "Optimizing Scheduling Problems in Cloud Computing Using a Multi-Objective Improved Genetic Algorithm," *2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE)*, Gurugram, India, 2025, pp. 635-640, doi: 10.1109/MRIE66930.2025.11156406.
29. L. C. Kasireddy, H. P. Bhupathi, R. Shrivastava, P. K. Sholapurapu, N. Bhatt and Ratnamala, "Intelligent Feature Selection Model using Artificial Neural Networks for Independent Cyberattack Classification," *2025 2nd International Conference On Multidisciplinary Research and*

Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 572-576, doi: 10.1109/MRIE66930.2025.11156728.

30. Prem Kumar Sholapurapu. (2025). AI-Driven Financial Forecasting: Enhancing Predictive Accuracy in Volatile Markets. European Economic Letters (EEL), 15(2), 1282–1291. https://doi.org/10.52783/eel.v15i2.2955
31. S. Jain, P. K. Sholapurapu, B. Sharma, M. Nagar, N. Bhatt and N. Swaroopa, "Hybrid Encryption Approach for Securing Educational Data Using Attribute-Based Methods," 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, Raigarh, India, 2025, pp. 1-6, doi: 10.1109/OTCON65728.2025.11070667.
32. Devasenapathy, Deepa. Bhimaavarapu, Krishna. Kumar, Prem. Sarupriya, S.. Real-Time Classroom Emotion Analysis Using Machine and Deep Learning for Enhanced Student Learning. Journal of Intelligent Systems and Internet of Things , no. (2025): 82-101. DOI: https://doi.org/10.54216/JISIoT.160207
33. Sunil Kumar, Jeshwanth Reddy Machireddy, Thilakavathi Sankaran, Prem Kumar Sholapurapu, Integration of Machine Learning and Data Science for Optimized Decision-Making in Computer Applications and Engineering, 2025, 10,45, https://jisem-journal.com/index.php/journal/article/view/8990
34. Prem Kumar Sholapurapu. (2024). Ai-based financial risk assessment tools in project planning and execution. European Economic Letters (EEL), 14(1), 1995–2017. https://doi.org/10.52783/eel.v14i1.3001
35. S. Kumar, "Multi-Modal Healthcare Dataset for AI-Based Early Disease Risk Prediction," IEEE Dataport, 2025, doi: 10.21227/p1q8-sd47
36. S. Kumar, "FedGenCDSS Dataset For Federated Generative AI in Clinical Decision Support," IEEE Dataport, Jul. 2025, doi: 10.21227/dwh7-df06
37. S. Kumar, "Edge-AI Sensor Dataset for Real-Time Fault Prediction in Smart Manufacturing," IEEE Dataport, Jun. 2025, doi: 10.21227/s9yg-fv18
38. S. Kumar, P. Muthukumar, S. S. Mernuri, R. R. Raja, Z. A. Salam, and N. S. Bode, "GPT-Powered Virtual Assistants for Intelligent Cloud Service Management," 2025 IEEE Smart Conference on Artificial Intelligence and Sciences (SmartAIS), Honolulu, HI, USA, Oct. 2025, doi: 10.1109/SmartAIS61256.2025.11198967
39. S. Kumar, A. Bhattacharjee, R. Y. S. Pradhan, M. Sridharan, H. K. Verma, and Z. A. Alam, "Future of Human-AI Interaction: Bridging the Gap with LLMs and AR Integration," 2025 IEEE Smart Conference on Artificial Intelligence and Sciences (SmartAIS), Indore, India, Oct. 2025, doi: 10.1109/SmartAIS61256.2025.11199115
40. S. Kumar, "A Generative AI-Powered Digital Twin for Adaptive NASH Care," Commun. ACM, Aug. 27, 2025,10.1145/3743154
41. S. Kumar, M. Patel, B. B. Jayasingh, M. Kumar, Z. Balasm, and S. Bansal, "Fuzzy Logic-Driven Intelligent System for Uncertainty-Aware Decision Support Using Heterogeneous Data," J. Mach. Comput., vol. 5, no. 4, 2025, doi: 10.53759/7669/jmc202505205
42. S. Kumar, "Generative AI in the Categorisation of Paediatric Pneumonia on Chest Radiographs," Int. J. Curr. Sci. Res. Rev., vol. 8, no. 2, pp. 712–717, Feb. 2025, doi: 10.47191/ijcsrr/V8-i2-16
43. S. Kumar, "Generative AI Model for Chemotherapy-Induced Myelosuppression in Children," Int. Res. J. Modern. Eng. Technol. Sci., vol. 7, no. 2, pp. 969–975, Feb. 2025, doi: 10.56726/IRJMETS67323
44. S. Kumar, "Behavioral Therapies Using Generative AI and NLP for Substance Abuse Treatment and Recovery," Int. Res. J. Modern. Eng. Technol. Sci., vol. 7, no. 1, pp. 4153–4162, Jan. 2025, doi: 10.56726/IRJMETS66672
45. S. Kumar, "Early Detection of Depression and Anxiety in the USA Using Generative AI," Int. J. Res. Eng., vol. 7, pp. 1–7, Jan. 2025, 10.33545/26648776.2025.v7.i1a.65
46. S. Kumar, "A Transformer-Enhanced Generative AI Framework for Lung Tumor Segmentation and Prognosis Prediction," *J. Neonatal Surg.*, vol. 13, no. 1, pp. 1569–1583, Jan. 2024. [Online]. Available: https://jneonatalsurg.com/index.php/jns/article/view/9460
47. S. Kumar, "Adaptive Graph-LLM Fusion for Context-Aware Risk Assessment in Smart Industrial Networks," Frontiers in Health Informatics, 2024. [Online]. Available: https://healthinformaticsjournal.com/index.php/IJMI/article/view/2813
48. Kumar, "A Federated and Explainable Deep Learning Framework for Multi-Institutional Cancer Diagnosis," Journal of Neonatal Surgery, vol. 12, no. 1, pp. 119–135, Aug. 2023. [Online]. Available: https://jneonatalsurg.com/index.php/jns/article/view/9461
49. S. Kumar, "Explainable Artificial Intelligence for Early Lung Tumor Classification Using

Hybrid CNN-Transformer Networks," *Frontiers in Health Informatics*, vol. 12, pp. 484–504, 2023. [Online]. Available: https://healthinformaticsjournal.com/downloads/files/2023-484.pdf

50. Varadala Sridhar,Dr.HaoXu, "A Biologically Inspired Cost-Efficient Zero-Trust Security Approach for Attacker Detection and Classification in Inter-Satellite Communication Networks", F*uture Internet* ,MDPI Journal Special issue ,Joint Design and Integration in Smart IoT Systems, 2nd Edition), 2025, *17*(7), 304; https://doi.org/10.3390/fi17070304, 13 July 2025
51. Varadala Sridhar, Dr.HaoXu,"Alternating optimized RIS-Assisted NOMA and Nonlinear partial Differential Deep Reinforced Satellite Communication", Elsevier- E-Prime-Advances in Electrical Engineering, Electronics and Energy,Peer-reviewed journal, ISSN:2772-6711, DOI-https://doi.org/10.1016/j.prime.2024.100619,29th may, 2024.
52. Varadala Sridhar,Dr.S.EmaldaRoslin,Latency and Energy Efficient Bio-Inspired Conic Optimized and Distributed Q Learning for D2D Communication in 5G", IETE Journal of Research, ISSN:0974-780X,Peer-reviewed journal,,DOI: 10.1080/03772063.2021.1906768 , 2021, Page No: 1-13, Taylor and Francis
53. V.Sridhar, K.V. Ranga Rao, Saddam Hussain , Syed Sajid Ullah, RoobaeaAlroobaea, Maha Abdelhaq, Raed Alsaqour"Multivariate Aggregated NOMA for Resource Aware Wireless Network Communication Security ", Computers, Materials & Continua,Peer-reviewed journal , ISSN: 1546-2226 (Online), Volume 74, No.1, 2023, Page No: 1694-1708, https://doi.org/10.32604/cmc.2023.028129,TechSciencePress
54. Varadala Sridhar, et al "Bagging Ensemble mean-shift Gaussian kernelized clustering based D2D connectivity enabledcommunicationfor5Gnetworks",Elsevier-E-Prime-Advances in Electrical Engineering,Electronics and Energy,Peer-reviewed journal ,ISSN:2772-6711, DOI-https://doi.org/10.1016/j.prime.2023.100400,20 Dec, 2023.
55. Varadala Sridhar, Dr.S.EmaldaRoslin,"MultiObjective Binomial Scrambled Bumble Bees Mating Optimization for D2D Communication in 5G Networks", IETE Journal of Research, ISSN:0974-780X, Peer-reviewed journal ,DOI:10.1080/03772063.2023.2264248 ,2023, Page No: 1-10, Taylor and Francis.
56. Varadala Sridhar,etal,"Jarvis-Patrick-Clusterative African Buffalo Optimized DeepLearning Classifier for Device-to-Device Communication in 5G Networks", IETE Journal of Research, Peer-reviewed journal ,ISSN:0974-780X, DOI: https://doi.org/10.1080/03772063.2023.2273946 ,Nov 2023, Page No: 1-10,Taylor and Francis
57. 57.V.Sridhar,K.V.RangaRao,V.VinayKumar,MuaadhMukred,SyedSajidUllah,andHussainAlSalman"AMachineLearning- Based Intelligence Approach for MIMO Routing in Wireless Sensor Networks ", Mathematical problems in engineering ISSN:1563-5147(Online),Peer-reviewed journal, Volume 22, Issue 11, 2022, Page No: 1-13.https://doi.org/10.1155/2022/6391678
58. VaradalaSridhar, Dr.S.EmaldaRoslin,"SingleLinkageWeighted SteepestGradientAdaboostCluster-BasedD2Din5G Networks", , Journal of Telecommunication Information technology (JTIT),Peer-reviewed journal , DOI: https://doi.org/10.26636/jtit.2023.167222, March (2023).

