S & M 4144

IoT-driven Dynamic Risk Management in Supply Chain Finance: A Multitechnology Fusion Framework and Collaborative Implementation Strategies

Linjing Liu,[1,2*] Yushi Chen,[3] Jia Yang,[4] and Cheng-Fu Yang[5,6**]

[1]Nottingham University Business School, University of Nottingham Malaysia, Selangor 43500, Malaysia
[2]Business School, Dongguan City University, Guangdong 523419, China
[3]School of Economics and Management, Dongguan University of Technology, Guangdong 523106, China
[4]Guangdong-Taiwan College of Industrial Science and Technology, Dongguan University of Technology, Guangdong 523106, China
[5]Department of Chemical and Materials Engineering, National University of Kaohsiung, Kaohsiung 811, Taiwan
[6]Department of Aeronautical Engineering, Chaoyang University of Technology, Taichung 413, Taiwan

(Received June 5, 2025; accepted July 14, 2025)

Keywords: IoT, risk management, supply chain finance, multitechnology fusion framework, collaborative implementation strategies

Supply chain finance (SCF) plays a key role in easing financing difficulties for small and medium-sized enterprises, but it also comes with risks such as information asymmetry, fraud involving pledged assets, and delays in credit evaluation. In this study, we introduce a dynamic risk management framework driven by IoT and enhanced by the integration of multiple technologies. Built on a four-layer IoT structure, comprising perception, network, processing, and application layers, the framework combines blockchain for secure and trusted data sharing, federated learning for collaborative data processing, and digital twin models for real-time risk simulation. At the perception level, 5th-Generation Mobile Communication Technology (5G)-enabled low-power sensors ensure comprehensive and tamper-proof data collection. The network layer uses blockchain techniques such as sharding and zero-knowledge proofs to safeguard data privacy and institutional trust. In the processing layer, federated learning combined with edge and cloud computing enhances credit evaluation. On the other hand, the application layer employs smart contracts and feedback mechanisms to enable real-time responses and adaptive risk strategies. To put this framework into practice, we propose a phased approach: first building a real-time data ecosystem, then deploying secure risk control systems, optimizing distributed computing, and finally integrating a closed-loop risk control mechanism. This modular, collaborative strategy ensures that technological systems align with actual business needs. Ultimately, the research demonstrates how IoT, blockchain, and AI can work together to create a scalable and practical model for managing risk dynamically in SCF.

[*]Corresponding author: e-mail: saxll5@nottingham.edu.my
[**]Corresponding author: e-mail: cfyang@nuk.edu.tw

https://doi.org/10.18494/SAM5788

1. Introduction

In recent years, supply chain finance (SCF) has become an essential tool for improving global capital flow efficiency and easing the financing difficulties faced by small and medium-sized enterprises (SMEs). This financial model has gained importance in supporting international trade and promoting coordination across industries.(1,2) However, according to the International Finance Corporation (IFC), the global financing gap for SMEs still stands at a staggering $5.5 trillion USD as of 2024. This shortfall is particularly severe in developing economies, where issues like information asymmetry and inadequate credit assessment methods pose significant barriers to SME financing.(3,4) While the global SCF market reached $75.3 billion USD in 2024 and is projected to grow to $152.2 billion USD by 2033 with a compound annual growth rate (CAGR) of 8.08%,(5) SME participation remains below 25%. This low adoption rate highlights the pressing need for technology-driven risk management solutions that can better support the evolving financial demands of global supply chains. The rapid integration of IoT, blockchain, and AI technologies offers transformative potential for improving risk management in SCF.

As reported by IoT Analytics in late 2024, global commercial IoT connections are expected to rise from 1.13 billion in 2020 to 4.11 billion by 2030, with a CAGR of approximately 13.8%, as shown in Fig. 1. This growth reflects the increasing use of real-time monitoring in areas such as warehousing and logistics, laying a solid technical foundation for enhanced data acquisition and transparency in SCF operations. Despite this progress, much of the existing research tends to examine these technologies in isolation, such as using blockchain for verification or big data for credit scoring, without fully exploring the benefits of integrating them. For example, IoT can support the real-time tracking of pledged assets,(6) but weak data privacy protections may raise concerns about confidentiality. Likewise, while blockchain can build decentralized trust systems,(7) its current performance limitations may hinder the real-time responsiveness needed for effective dynamic risk management. One of the key engineering challenges in SCF today is optimizing the entire process chain, from trustworthy data collection and secure, privacy-

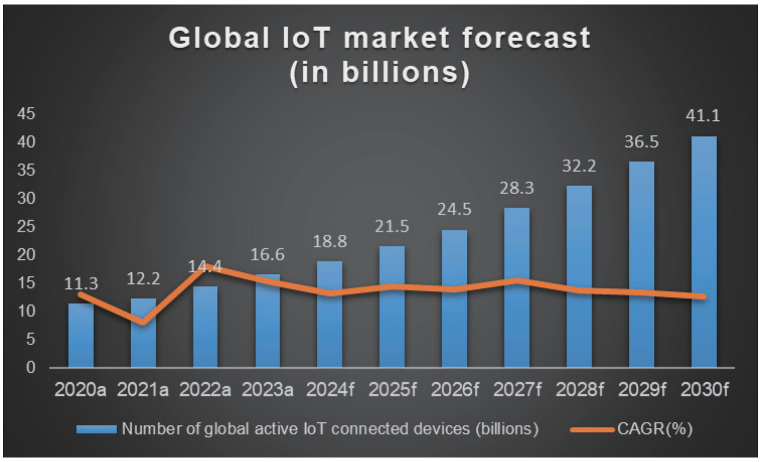

Fig. 1. (Color online) Global IoT market forecast in billions (modified from IoT Analytics, 2024).

preserving sharing to intelligent, real-time decision-making, through the convergence of emerging technologies.

The primary challenge in current SCF risk management lies in the over-reliance on anchor enterprise credit and static historical data for credit assessment. This approach fails to reflect the real-time operational status of SMEs.(8,9) Additionally, financial institutions lack the capability to integrate full-chain data in real time, leading to biased credit models and suboptimal lending decisions. Owing to limited credit transparency, around 40% of SMEs in developing countries are excluded from formal financing channels, and approved credit limits often fall short of actual needs. Furthermore, the decoupling of logistics and fund flow data reduces the ability to verify transaction authenticity, making it harder to detect fabricated trades or fake warehouse receipts. This significantly increases both default risk and financing costs. In dynamic collateral scenarios, high-liquidity and high-volatility assets are prone to risks such as duplicate pledging if not monitored in real time. Traditional methods relying on manual checks and offline data cannot respond promptly. During storage and transportation, the lack of continuous tracking of inventory changes, cargo condition, and transit routes leads to growing risks of asset depreciation and loss of control.

In practice, traditional SCF risk management relies heavily on manual processes and fragmented tools, resulting in low efficiency and limited scalability, especially when dealing with a large number of SMEs. For example, monitoring collateral during storage and transport often depends on manual checks and paper-based tracking, which are error-prone and time-consuming. At the same time, the lack of standardized interfaces among financial, logistics, and regulatory systems creates fragmented data flows, making it difficult for financial institutions to monitor supply chain activity in real time. Data sharing across organizations is also hindered by privacy concerns and trade secrets. Current data anonymization methods often struggle to balance privacy protection with usability, reducing collaboration efficiency. These issues frequently lead to delays and high dispute resolution costs. Worse still, centralized data architectures are vulnerable to cyberattacks, and data breaches are increasingly common. Fundamentally, the main issue in SCF is the gap between slow, outdated risk management approaches and the fast-moving nature of modern supply chains. Information asymmetry makes it difficult to detect issues with collateral in time, and repeated pledging or fraud is common. Data silos and fragmented risk control further increase credit assessment errors and slow down response times. Improving real-time risk monitoring and cross-party collaboration is key to the sustainable development of SCF.

In this study, we integrated approach demands not only overcoming the limitations of individual technologies but also harnessing their complementary strengths to build systems that are secure, robust, and efficient. Developing such multitechnology solutions requires thoughtful architectural design, adherence to interoperability standards, and practical implementation strategies to meet the complex needs of global supply chains. In this research, we address both theoretical and practical gaps by proposing an IoT-driven, multitechnology integration framework for dynamic risk management. By systematically combining a four-layer IoT architecture (including perception, network, processing, and application layers) with blockchain-based distributed ledgers,(10,11) federated learning for collaborative computation, and digital twin modeling for real-time simulation, the proposed framework offers a comprehensive solution to longstanding challenges in SCF, such as fragmented data, dynamic fraud, and delayed risk response.

In this research, we introduce several innovative engineering solutions that enhance risk management in SCF through integrated technologies. One major contribution is the development of a dynamic asset digitalization protocol (DADP), which uses IoT data to build digital twin models of pledged assets.(12,13) This allows for dynamic asset valuation and the real-time detection of anomalies with greater accuracy. Another key advancement is the creation of a privacy-preserving cross-validation (PPCV) mechanism, which applies zero-knowledge proofs (ZKPs) to enable secure data sharing between institutions. This balances the need for collaborative analysis with the protection of sensitive information. Additionally, we design an edge-cloud federated learning model that improves the adaptability and accuracy of credit scoring systems when working with diverse and decentralized data sources. On a theoretical level, we demonstrate the synergistic benefits of combining IoT, blockchain, and AI technologies, proposing a new risk management model that is dynamic, collaborative, and distributed, moving beyond traditional static methods. From a practical perspective, the framework offers a phased implementation strategy that supports scalable digital transformation for financial institutions and SMEs, tailored to varying levels of technological readiness and resource availability. Overall, the research result of this work not only enriches theoretical insights into integrated systems but also offers practical tools to strengthen financial risk management in complex supply chain environments.

We begin by reviewing the evolution of risk management in SCF, focusing on how technological convergence has shaped modern financial engineering. We outline the shift from traditional credit-based methods to data-driven systems, and eventually to today’s integrated, technology-enabled approaches. This historical perspective helps contextualize how emerging technologies have begun to address long-standing issues in global supply chain risk management. Building on this foundation, we examine current challenges in SCF, particularly the problem of information asymmetry between financial institutions and supply chain actors, which highlights the need for more effective, technology-driven solutions. To address these challenges, we propose a new theoretical framework based on a four-layer IoT architecture, covering perception, network, processing, and application layers. Each layer incorporates technologies such as blockchain, federated learning, and digital twins, working together to support coordinated, comprehensive risk management. We also consider how these systems can be implemented flexibly across different organizational contexts, with a focus on key engineering concerns such as interoperability, efficiency, and resilience. In conclusion, in this work, we offer both theoretical insight and practical strategies for improving risk management in SCF. This also points to future directions, including a better integration of technologies, responsiveness to regulatory changes, and broader applications in supply chain management.

2. Theoretical Framework for SCF Risk Management Based on IoT Infrastructure

To address the aforementioned challenges, we propose a theoretical framework based on the four-layer architecture of IoT, comprising the perception, network, processing, and application layers. By leveraging cross-layer technological integration, the framework systematically enhances data reliability, strengthens privacy protection, and improves the efficiency of dynamic decision-making.

2.1 Overview of IoT

IoT refers to a networked paradigm that leverages intelligent sensing technologies to connect physical objects to the Internet for information exchange and communication.(14) Through contractual protocols, IoT enables intelligent identification, tracking, and regulation, thereby fostering a deep integration between the physical and digital worlds.(15) The fundamental technological architecture of IoT comprises the following four hierarchical layers:

1) Perception layer: This layer digitizes physical objects by collecting real-time environmental data, such as location, temperature and humidity, and vibration frequency, through technologies including sensors, radio frequency identification (RFID), and GPS.
2) Network layer: Utilizing advanced communication technologies [e.g., 5th-Generation Mobile Communication Technology (5G), low-power wide-area network (LPWAN)] and standard protocols (e.g., TCP/IP), this layer ensures efficient data transmission and interoperability across heterogeneous systems.
3) Processing layer: At this level, edge and cloud computing processes are employed to cleanse, analyze, and model data, extracting actionable insights.
4) Application layer: This top layer transforms processed data into executable decisions and services via user interfaces and business logic.

As illustrated in Fig. 2, this framework emphasizes the vertical integration of core IoT technologies, thereby providing a foundational infrastructure for subsequent technological convergence.(16)

2.2 Perception layer: hybrid sensing and trusted data sources

The perception layer acts as the “sensory system” of IoT. Its core role is to digitally map physical assets with high accuracy across various environments using multidimensional sensing technologies, providing reliable input for upper-level systems. In traditional SCF, risks such as duplicate pledging, cargo tampering, and outdated asset valuation often stem from weak data collection at the perception layer. For example, in static warehouse environments, manual inspections or single sensors cannot effectively cover large areas, leading to delayed data updates. In dynamic transport scenarios, insufficient tracking makes it difficult to detect route deviations or tampering, creating blind spots that increase fraud risk and information asymmetry for financial institutions. To address these issues, the perception layer must integrate multiple sensing technologies. For instance, in warehouse settings, RFID systems can periodically scan

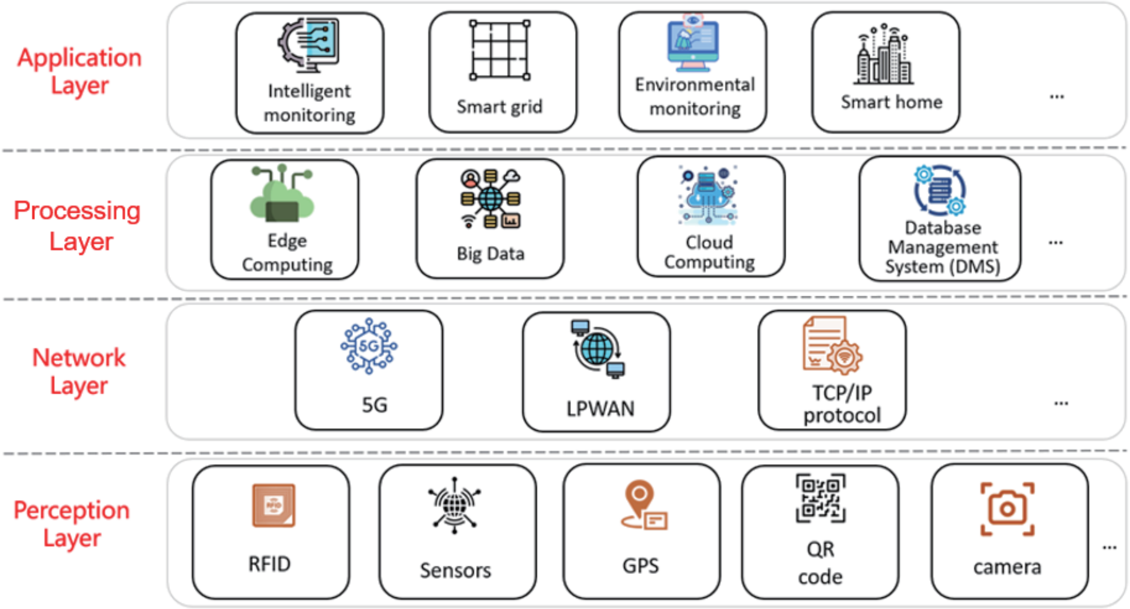

Fig. 2. (Color online) Architecture diagram of IoT.

tagged items to update inventory in real time. These readings can be cross-checked with environmental sensors such as temperature and humidity monitors to detect abnormal movement or counterfeit tags. In addition, deploying a multisensor network helps eliminate blind spots in static environments by periodically collecting environmental data from various sensors. For moving assets, transport vehicles can be equipped with high-precision GPS modules and three-axis accelerometers to monitor location and cargo vibration. This provides both geospatial and physical anchoring for dynamic collateral monitoring. At the core of this sensing layer is DADP, a key innovation. DADP uses real-time IoT data to build a digital twin of the pledged asset, combining physical parameters (location or environmental conditions) with market data (e.g., futures prices and storage costs) to continuously calculate the asset's real-time value. The main breakthrough of DADP is shifting from static valuation to a dynamic, data-driven process.

2.3 Network layer: distributed trust and privacy protection

The network layer acts as the "nervous system" of IoT, responsible for efficient data transmission and cross-organizational coordination. In traditional SCF, data silos and privacy risks often stem from limited communication capabilities and centralized architectures. For example, logistics delays cannot trigger financial responses in real time, leading to late credit freezes and increased default risk. At the same time, sharing sensitive data raises concerns about leaks of trade secrets. To address these challenges, the network layer adopts a hybrid approach using 5G and LPWAN, combined with blockchain sharding and cross-chain protocols to build a distributed trust system.(17,18) In dynamic transport scenarios, 5G enables high-bandwidth, low-latency transmission, allowing the real-time synchronization of high-frequency data such as

GPS locations and vibration metrics. This ensures that financial institutions can continuously monitor the condition of pledged assets. LPWAN is mainly used in static warehouse environments to enable wide coverage and energy-efficient data transmission. It supports periodic updates from temperature and humidity sensors while significantly reducing maintenance costs. Blockchain sharding separates logistics and financial data into distinct storage channels, allowing parallel processing to improve system throughput, an essential feature for high-frequency transactions in SCF. Cross-chain protocols further enable interoperability between different blockchain networks. By using event-driven mechanisms, they allow real-time coordination between logistics and financial systems. A key innovation at the network layer is PPCV. This module leverages ZKP technology,(19) allowing financial institutions to verify specific claims, such as "inventory ≥ contract threshold", without accessing the raw data. PPCV protects sensitive information while enabling trusted collaboration between multiple parties, laying the technical foundation for cross-institutional risk control.

2.4 Processing layer: collaborative computing and intelligent decision-making

The processing layer serves as the "decision center" of IoT systems, handling massive data cleaning, analysis, and modeling to support dynamic risk assessment. Traditional SCF relies on centralized data processing, facing challenges in credit evaluation bias and insufficient model generalization, primarily due to limited data processing capabilities. SMEs often receive distorted credit scores owing to missing data, while the noise data collected from edge devices (such as logistics vibration interference) further weaken model accuracy. Additionally, static models struggle to adapt to external shocks such as market fluctuations, resulting in delayed risk assessments. To address these issues, the processing layer implements edge computing and federated learning technologies to build a collaborative computing framework. Edge computing deploys servers at key supply chain nodes (such as warehouses and transport vehicles) to clean local data in real time (filtering vibration noise, for example) and extract valuable features before cloud transmission. This layered computing architecture reduces data transmission load while improving response time.

Federated learning enables various participants (core enterprises, logistics companies, and financial institutions) to train local submodels, sharing encrypted parameters that are aggregated in the cloud to generate comprehensive credit scores. This approach protects data privacy while enhancing model generalization capabilities. The risk prediction digital twin represents the core innovation module within the processing layer. By integrating real-time IoT data with historical transaction records, this module simulates extreme scenarios and dynamically outputs default probabilities along with response strategies. This transforms traditional static risk assessment into a dynamic simulation process, strengthening the system's resilience against extreme events. The dynamic modeling functions in the perception layer's DADP (such as market fluctuation predictions) must work together with the digital twin in the processing layer, creating a closed loop from real-time data anchoring to risk assessment.

2.5 Application layer: adaptive risk control and closed-loop optimization

The application layer serves as the "service interface" of IoT systems, transforming processed data into executable business rules to achieve real-time risk response and system self-optimization. Traditional SCF risk control relies on manual rules and after-the-fact processing, with response speeds failing to match the dynamic changes in supply chains. For example, when inventory levels decrease, manual approval for credit adjustments creates risk delays. The lack of cross-institutional risk collaboration mechanisms further weakens the overall risk control efficiency. These response delays and inefficient manual interventions stem primarily from deficiencies in the application layer. The application layer can build an adaptive risk control loop through smart contracts and cross-layer feedback mechanisms. Smart contracts automatically trigger operations on the basis of inputs from the perception and processing layers (such as inventory pledge rates and credit scores) according to preset rules. The AI-blockchain risk dashboard integrates multisource data (including RFID status, federated scoring, and digital twin prediction results) and uses a visualization interface to mark risk levels in real time (red/yellow/green lights), helping decision-makers quickly identify problems and develop intervention strategies.

The cross-layer feedback loop represents the core innovation of the application layer. When risk events (such as duplicate pledge alerts) are detected at the application layer, this triggers adjustments in the perception layer's monitoring strategies (such as increasing RFID scanning frequency). Simultaneously, historical risk data feed back to the processing layer to optimize weight allocation in federated learning models. This creates an adaptive cycle of "monitoring-response-iteration" that gives the system self-evolving capabilities. The continuous flow of information across layers enables the system to learn from past incidents and automatically refine its operations, making the entire framework more resilient and responsive to emerging risks. The IoT four-layer architecture creates a complete chain from data collection to risk response through layered collaboration and closed-loop feedback, as shown in Fig. 3. The perception layer ensures data trustworthiness, while the network layer guarantees privacy and collaboration efficiency. The processing layer enhances decision-making intelligence, and the application layer enables dynamic adaptability.

3. Implementation Pathway and Outcomes of SCF Risk Management Based on IoT Infrastructure

Building upon the technological foundation laid out in the preceding sections, we propose a theoretical framework that undergirds a comprehensive approach to risk management in SCF. The integration of technologies within this framework is not merely conceptual but is directed toward practical realization through an engineering-focused implementation strategy. By adopting a phased deployment process, we translate abstract theoretical constructs into actionable practices, enabling full-spectrum management from data ecosystem development to multilayer feedback optimization. The implementation pathway is structured around four key

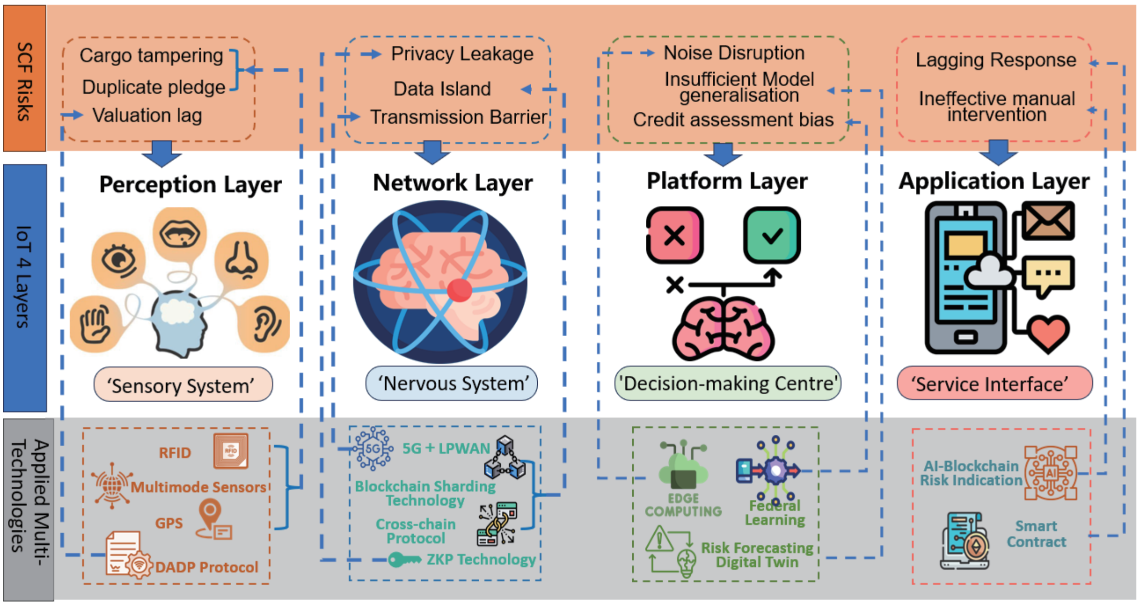

Fig. 3. (Color online) SCF risk management chain based on IoT structure.

objectives: full-scenario coverage, privacy-preserving trust, dynamic evaluation, and adaptive optimization.

3.1 Data environment development: constructing a real-time, scenario-integrated data ecosystem

The inherent complexity of SCF necessitates the continuous and comprehensive monitoring of collateral throughout its entire lifecycle. Traditional data collection methods, however, often result in fragmented monitoring, particularly between static warehousing conditions and dynamic transportation processes, thereby creating data blind spots and delaying responsive interventions. This phase addresses such limitations by employing IoT technologies to establish seamless, real-time data coverage across all operational scenarios. The objective is to ensure complete transparency in the status of pledged assets, thereby furnishing a highly reliable data foundation that supports dynamic and responsive risk control mechanisms, as illustrated in Fig. 4. In this study, we adopted a phased implementation approach for data acquisition.

Phase one focuses on data collection and transmission through the integration of RFID and GPS technologies to achieve comprehensive scenario coverage. In static warehousing environments, RFID tags and multimodal sensor networks are deployed. Each pledged asset is embedded with a unique RFID identifier, and temperature-humidity sensors are installed in storage areas. Periodic data collection (every 10 min) ensures transparency in inventory status. For dynamic transportation scenarios, where high-frequency data are required, transport vehicles are equipped with multimodal sensors, including high-precision GPS modules (updated per second), triaxial accelerometers (sampling rate of 100 Hz), and environmental sensors.

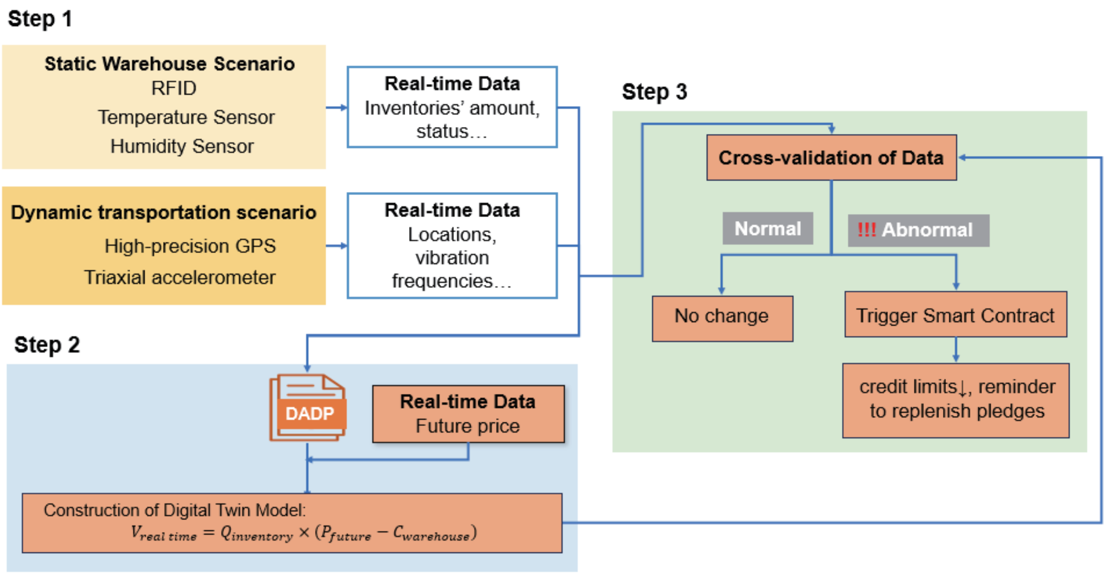
Step 1
Static Warehouse Scenario
RFID
Temperature Sensor
Humidity Sensor
Real-time Data
Inventories' amount, status…
Dynamic transportation scenario
High-precision GPS
Triaxial accelerometer
Real-time Data
Locations, vibration frequencies…
Step 2
DADP
Real-time Data
Future price
Construction of Digital Twin Model:
$V_{real\ time} = Q_{inventory} \times (P_{future} - C_{warehouse})$
Step 3
Cross-validation of Data
Normal
!!! Abnormal
No change
Trigger Smart Contract
credit limits↓, reminder to replenish pledges

Fig. 4. (Color online) Real-time data ecosystem of supply chain with full scene coverage.

Phase two emphasizes the development of a digital twin model to enable the dynamic valuation of pledged assets. DADP integrates physical parameters (e.g., inventory quantity and location) with market data (e.g., commodity futures prices) to construct a digital twin. The real-time value of pledged assets is calculated using the following formula:

$$V_{real\text{-}time} = Q_{inventory} \times (P_{futures} - C_{storage}), \tag{1}$$

where $V_{real\text{-}time}$ denotes the real-time market value of the pledged asset, $Q_{inventory}$ is the actual physical quantity in storage or transit, $P_{futures}$ is the real-time futures market price of the asset, and $C_{storage}$ represents the unit storage cost, including fees for custody, insurance, and potential losses.

Phase three implements an automated risk response mechanism, activated through the cross-validation of multisource data. For example, if a vibration sensor detects abnormal activity while the RFID tag location remains unchanged, the system infers possible tag tampering or asset substitution and immediately freezes related financing. Similarly, if the futures price drops beyond a predefined threshold, a smart contract automatically reduces the credit limit and prompts the enterprise to provide additional collateral. This mechanism significantly shortens the traditional manual approval process, from several days to just minutes, minimizing delays due to human intervention and reducing the risk of under-collateralization caused by market volatility. It also enhances the real-time risk management capabilities of financial institutions.

The integration of RFID and GPS effectively addresses the heterogeneous requirements of static and dynamic scenarios. Sensor fusion validation, through logical consistency analysis (e.g., matching vibration data with spatiotemporal trajectories), significantly enhances antitampering capabilities. Moreover, DADP enables dynamic mapping between physical assets and their financial value via digital twin technology.

3.2 Secure risk control environment: privacy protection and automated response

Cross-institutional collaboration is a defining feature of SCF, yet data silos and privacy risks hinder coordination among stakeholders. This phase aims to establish a distributed trust framework using blockchain and cryptographic technologies, enabling secure data sharing while preserving privacy. This ensures efficient collaboration among logistics, financial, and regulatory entities, as illustrated in Fig. 5. The first step focuses on data authentication and hybrid networking by integrating LPWAN and 5G technologies with a blockchain sharding architecture to achieve reliable, multiparty data storage.

1) Static warehousing scenario: A LPWAN sensor network is deployed to support large-scale, energy-efficient data collection. For example, in a grain storage facility, temperature and humidity sensors update environmental data every 10 min and transmit it to the cloud via LPWAN. If humidity exceeds a safety threshold, the system automatically activates dehumidifiers to prevent mold formation. The extensive coverage and long battery life of LPWAN make it ideal for large warehouse environments, significantly reducing operational costs.
2) Dynamic transportation scenario: A 5G-based edge computing solution is applied, where industrial 5G gateways transmit real-time data to edge servers. These edge nodes analyze features such as vibration patterns and route deviations locally. For instance, if a vehicle exhibits abnormal vibration frequencies, the edge server flags a potential cargo damage risk and triggers a local alert. This avoids response delays that may occur owing to reliance on cloud-based processing.

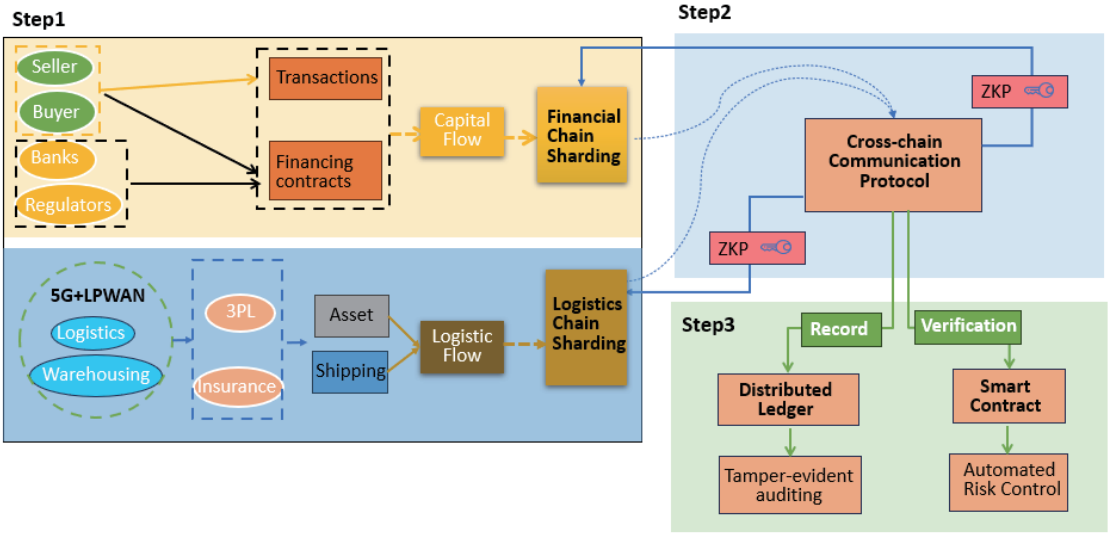

Fig. 5. (Color online) SCF security risk control environment workflow.

3) Blockchain sharding architecture: The logistics chain can be built on a consortium blockchain, such as Hyperledger Fabric, maintained by nodes operated by third-party logistics providers and insurance companies.(20) These nodes are responsible for storing hashed proofs of key data, including cargo trajectories and environmental conditions. In parallel, the financial chain can utilize a high-performance public blockchain, such as Ethereum 2.0, with nodes maintained by banks and regulatory agencies to record credit scores and contract terms. Sharding architecture enables parallel processing, significantly improving throughput and meeting the demands of high-frequency transactions.

Phase two focuses on cross-chain verification and privacy protection, enabling interoperability between heterogeneous blockchains and secure data validation through cross-chain protocols and ZKPs.

1) Event-driven cross-chain synchronization: A cross-chain communication protocol (e.g., Cosmos) connects the logistics and financial blockchains. Critical events, such as shipment delays exceeding 48 h or environmental threshold violations, are synchronized across chains to trigger predefined smart contracts.(20) For instance, upon detecting a logistics delay, the financial blockchain automatically reduces the credit limit within a specified timeframe and logs the action in an immutable distributed ledger.
2) Privacy-preserving verification: When financial institutions need to verify claims (e.g., “customs documents are valid and inventory meets the contractual threshold”), the logistics provider submits encrypted hash values instead of raw data. For example, to prove that inventory $\geq$ 1000 units, the logistics chain stores a hashed record such as “0x3a7b”. The financial chain uses ZKP to confirm compliance without revealing exact figures. This approach addresses the inefficiencies of traditional inter-institutional processes by enabling timely, privacy-preserving validation.

Phase three deploys automation in execution and audit traceability, leveraging smart contracts and distributed ledgers to enable rule-based rapid risk response and full process transparency.

1) Automated risk control execution: Predefined conditions, such as a 10% inventory drop or a deviation of more than 50 km from the logistics route, trigger smart contract actions. For example, when inventory drops below the threshold, the contract automatically freezes a portion of the payment and notifies the enterprise to replenish stock. Similarly, if the logistics path deviates, an insurance claim process is triggered, and the credit status is updated in real time.
2) Immutable auditing: All operational records, such as credit adjustments or claims instructions, are recorded on the blockchain ledger, allowing regulatory authorities to trace the full lifecycle of events in real time.

The synergy of blockchain sharding, cross-chain protocols, and smart contracts establishes a fully automated risk control system covering the entire process, from evidence storage and verification to execution. This comprehensive automation not only enhances operational efficiency but also ensures robust transparency and accountability in risk management practices. As a result, financial institutions and other stakeholders benefit from improved decision-making and reduced latency in responses to operational risks.

3.3 Distributed multicenter system: collaborative computing and dynamic risk prediction

Traditional risk control models rely on static historical data, making them inadequate for addressing the dynamic nature of supply chains (e.g., market fluctuations and logistics disruptions). This phase aims to build an adaptive risk assessment framework through edge-cloud collaborative computing and federated learning. The goal is to enhance the model's generalization in complex scenarios and shift from reactive response to proactive prevention.

The first stage focuses on edge-level data preprocessing to address noise and real-time processing requirements. Edge computing devices are deployed at supply chain nodes (e.g., warehouses and transport vehicles) to filter noise and extract key features in real time. For example, edge servers installed on cold-chain transport vehicles can remove sensor noise caused by device heating and extract meaningful indicators such as average temperature fluctuation. High-risk event data (e.g., temperature breaches) are prioritized and transmitted to the cloud via 5G network slicing, ensuring the timely delivery of critical information while reducing transmission load and improving response speed, as shown in Fig. 6.

The second stage focuses on federated learning to overcome data silos while preserving data privacy. Core enterprises train a "production efficiency-repayment ability" submodel using production data (e.g., daily output and yield rate), while logistics providers train a "logistics timeliness-default risk" submodel using delivery performance data. Only encrypted model parameters are shared with the cloud. A global credit scoring model is then aggregated using the TensorFlow Federated framework, enhancing generalization while ensuring privacy protection, as shown in Fig. 7.

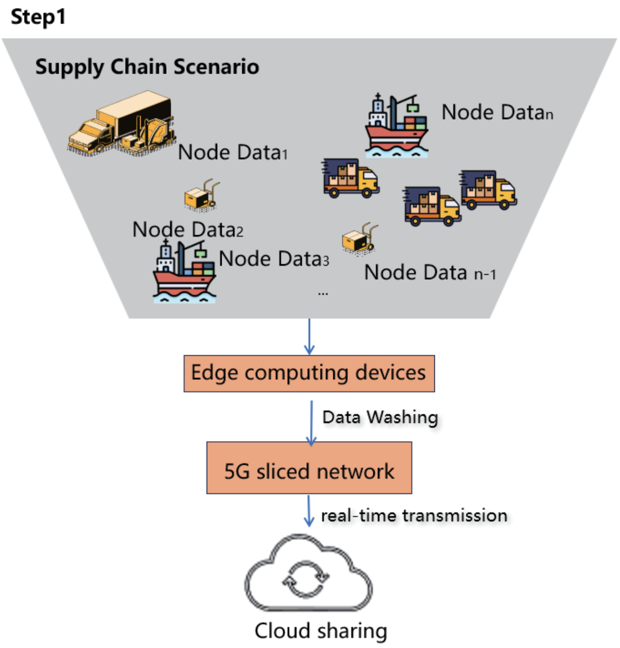

Fig. 6. (Color online) Edge data preprocessing workflow.

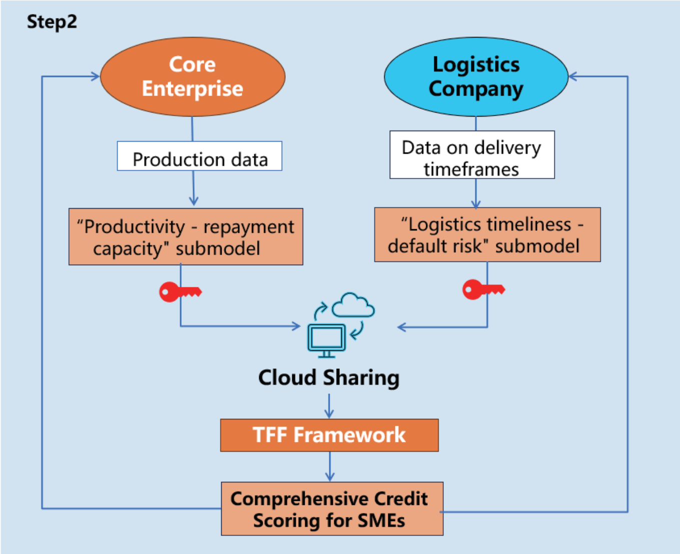
Step2
Core Enterprise
Logistics Company
Production data
Data on delivery timeframes
"Productivity - repayment capacity" submodel
"Logistics timeliness - default risk" submodel
Cloud Sharing
TFF Framework
Comprehensive Credit Scoring for SMEs

Fig. 7. (Color online) SCF federated learning model training workflow.

The third stage involves deploying dynamic risk assessment simulations to evaluate the impact of extreme scenarios on the supply chain. A digital twin for risk prediction integrates market data, policy data, and supply chain topology to construct a multidimensional simulation environment. For example, by inputting a hypothetical scenario such as "a 30-day port closure due to a pandemic," the digital twin can quantify the resulting logistics delays and their impact on the cash flow of upstream and downstream firms while also generating corresponding mitigation strategies (e.g., activating alternative logistics routes and adjusting credit priorities). This dynamic simulation capability enables a shift in risk control from reactive remediation to proactive prevention.

The integration of edge computing, federated learning, and digital twin technologies forms a progressive optimization loop, linking data, modeling, and simulation. Experimental results demonstrate that this coordinated approach significantly improves the accuracy of risk forecasts under volatile conditions and enhances the resilience of supply chain decision-making.

3.4 Collaborative risk control network: cross-institution coordination and feedback optimization

Traditional risk control relies on manual rules and post-incident responses, lacking cross-layer coordination mechanisms. This phase aims to establish an adaptive closed-loop system of "monitoring–response–iteration" through smart contracts and cross-layer feedback. The goal is to enable dynamic risk optimization and system self-learning. The phased implementation process is illustrated in Fig. 8.

The first stage focuses on real-time monitoring and visualization by integrating multisource data and labeling risk levels. An AI-blockchain-based risk dashboard is developed using

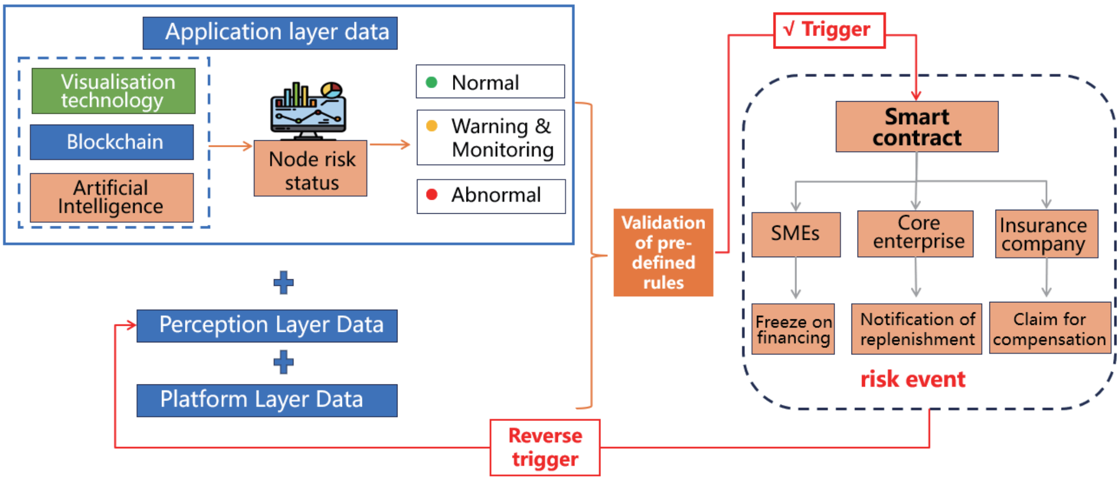

Fig. 8. (Color online) SCF risk synergy network flowchart.

visualization technologies such as D3.js to display the risk status of supply chain nodes (red/yellow/green indicators). This assists decision-makers in quickly identifying issues and formulating intervention strategies. For example, nodes marked in red owing to abnormal inventory levels can trigger audit processes, while yellow nodes activate early warning monitoring.

The second stage emphasizes automated cross-institution coordination through smart contracts, enabling multiparty collaborative responses. On the basis of data inputs from sensing and processing layers, predefined rules (inventory pledge ratio > 90% or delivery delay > 48 h) are verified to trigger contract actions. For instance, in a food supply chain, if the inventory pledge ratio exceeds the threshold, the smart contract automatically freezes 50% of the payment and notifies the core enterprise to replenish stock. Simultaneously, the contract sends a compensation request to the insurance company, initiating a pre-approval process. This mechanism significantly reduces delays caused by manual intervention and overcomes coordination barriers in traditional multidepartment operations.

The third stage implements cross-layer feedback and closed-loop optimization to enable system self-learning and policy iteration. A forward control mechanism pushes risk events identified at the application layer (e.g., duplicate collateralization) back to the sensing layer. For instance, if repeated collateral alerts are frequently triggered at a specific warehouse, the system automatically increases the RFID scanning frequency from once per hour to once every 10 min. The reverse feedback mechanism sends historical risk data to the processing layer to refine the weight allocation in the federated learning models.

The integration of AI dashboards, smart contracts, and cross-layer feedback enables the risk control system to continuously learn and adapt. Experimental validation shows that this approach reduces detection latency by 35% and improves early-warning accuracy by 28%, enhancing the overall responsiveness and resilience of supply chain risk management. In this

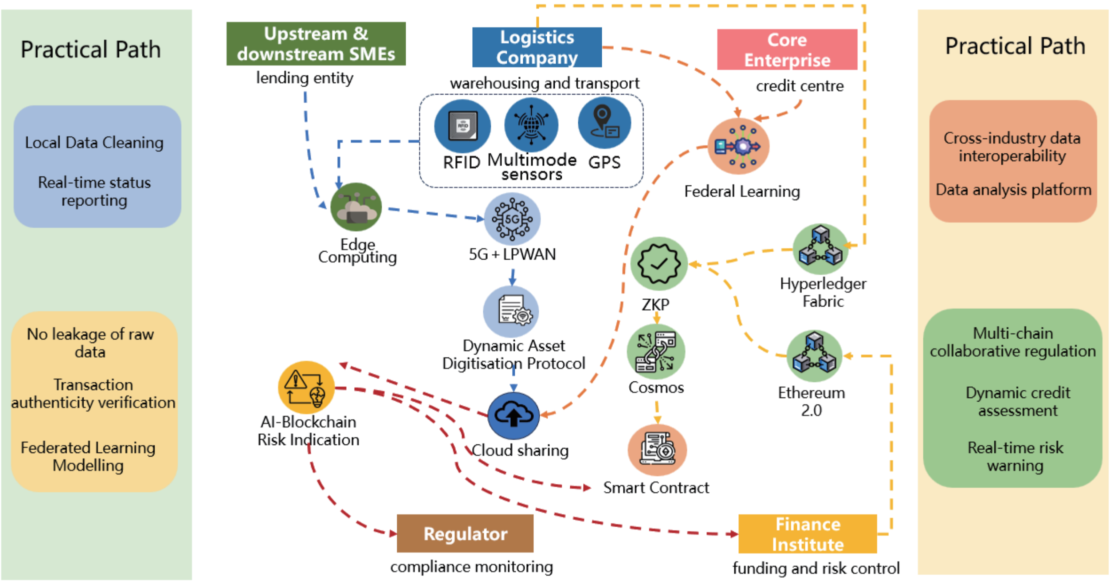

Fig. 9. (Color online) Risk management application scenarios for IoT SCF.

study, we successfully integrated cutting-edge technologies, namely, IoT, blockchain, AI, federated learning, and digital twin systems, to construct a dynamic and collaborative risk management framework for SCF. The proposed system effectively addresses key challenges such as information asymmetry, dynamic collateral fraud, and response latency. Empirical findings confirm that the synergistic application of these technologies enables trustworthy data acquisition, privacy-preserving information sharing, and intelligent dynamic decision-making, thereby achieving the end-to-end optimization of SCF risk management. This work offers an innovative paradigm for the digital transformation of SCF risk control, as illustrated in Fig. 9.

4. Conclusion

In this study, we integrated IoT with a suite of advanced technologies including blockchain, AI, federated learning, and digital twin systems. Specifically, blockchain technology, leveraging sharding architecture, and ZKP enabled trusted cross-institutional data interoperability while preserving privacy, effectively addressing the longstanding conflict between data silos and the risk of disclosing commercial secrets in traditional systems. The combination of federated learning with edge-cloud collaborative computing facilitated distributed parameter aggregation, thereby optimizing credit assessment models and significantly enhancing their adaptability to market volatility and supply chain dynamics. Digital twin technology, drawing on real-time IoT data, constructed the dynamic asset models that anchor collateral value in real time and provided early warnings of anomalies, thereby overcoming the limitations of static valuation methods. To overcome the performance bottlenecks inherent in centralized risk control systems, we proposed the development of a distributed and multicenter collaborative network. This network was driven by smart contracts, enabling automated responses and cross-layer feedback loops that together form a self-adaptive optimization cycle of monitoring, response, and iteration. The practical value of this study lied in its provision of a modular, phased pathway for digital transformation, offering financial institutions and SMEs a framework that encompassed the construction of real-time data ecosystems, the deployment of secure risk control environments, the optimization of collaborative computation, and the integration of closed-loop systems.

Acknowledgments

This research was supported by projects under Nos. NSTC 113-2622-E-390-001 and NSTC 113-2221-E-390-011.

References

1 M. L. Gelsomino, R. Mangiaracina, A. Perego, and A. Tumino: Int. J. Phys. Distrib. Logist. Manage. **46** (2016) 348.
2 C. Bals: J. Purchasing Supply Manage. **25** (2019) 105.
3 T. T. L. Chong, L. Lu, and S. Ongena: J. Banking Finance **37** (2013) 3412.
4 M. G. Veiga and J. A. McCahery: Eur. Bus. Organ. Law Rev. **20** (2019) 633.
5 Supply Chain Finance Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2024–2033. https://www.imarcgroup.com/supply-chain-finance-market (accessed May, 2024).
6 R. Wang, C. Yu, and J. Wang: IEEE Access **7** (2019) 110323.
7 G. Hall, P. Hutchinson, and N. Michaelas: Int. J. Econ. Bus. **7** (2000) 297.
8 L. Guo, J. Chen, S. Li, Y. Li, and J. Lu: Digital Commun. Networks **8** (2022) 576.
9 https://www.quicksettle.ai/post/how-is-technology-revolutionizing-supply-chain-financing (accessed July 2024).
10 Blockchain for IoT Systems: Concept, Framework and Applications, V. Sridhar, S. Rani, P. K. Pareek, P. Bhambri, and A. A. Elngar, Eds (Chapman and Hall/CRC, New York, 2024) 1st ed.
11 K. Aditya, S. Chakraborty, A. Dahire, A. Kumari, and M. Milanova: Blockchain, IoT, and AI Technologies for Supply Chain Management. D. V. Grover, D. B. B. Balusamy, D. M. Milanova, and D. A. Y. Felix Eds. (Apress, Berkeley, CA, 2024) Chap. Integrating Blockchain, IoT, and AI in Supply Chain Management.
12 P. Devisri, B. Jamalpur, S. F. C. Raj, K. Velusamy, A. K. V, and B. Jegajothi: 2025 8th Int. Conf. Trends in Electronics and Informatics (ICOEI, Tirunelveli, India, 2025) 122–127.
13 E. Candón, A. Crespo, A. Guillén, J. Gómez, and J. López: IFAC-PapersOnLine **58** (2024) 216.
14 J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami: Future Gener. Comput. Syst. **29** (2022) 1645.
15 H. Fu, G. Manogaran, K. Wu, M. Cao, S. Jiang, and A. Yang: Int. J. Inf. Manage. **50** (2020) 515.
16 W. A. Abbasi, Z. Wang, Y. Zhou, and S. Hassan: Int. J. Distrib. Sens. Netw. **15** (2019) 155014771987400.
17 F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, S. Stachtiaris, M. Pagoni, and N. P. Rachaniotis: Int. J. Prod. Res. **59** (2021) 5758.
18 V. Sathiya, K. Nagalakshmi, K. Raju, and R. Lavanya: Sci. Rep. **14** (2024) 21621.
19 X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng: IEEE Network **35** (2021) 198.
20 T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen: Compu. Ind. Eng. **154** (2021) 107130.