Mesopotamian journal of Cybersecurity
Vol. 5, No.2, **pp**. 735–769
DOI: https://doi.org/10.58496/MJCS/2025/044; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

Blockchain and Federated Learning in Edge-Fog-Cloud Computing Environments for Smart Logistics

Guma Ali [1,13 *], Adebo Thomas [1], Maad M. Mijwil [2,3,4], Kholoud Al-Mahzoum [5], Malik Sallam [6, 7,8], Ayodeji Olalekan Salau[9, 10], Ioannis Adamopoulos [11], Indu Bala[12], Aseed Yaseen Rashid Al-jubori [2]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

[3] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[4] *Faculty of Engineering, Canadian Institute of Technology, Albania*

[5] *Sheikh Jaber Al-Ahmad Al-Sabah Hospital, Ministry of Health, Kuwait City, Kuwait*

[6] *Department of Pathology, Microbiology and Forensic Medicine, School of Medicine, The University of Jordan, Amman, Jordan*

[7] *Department of Clinical Laboratories and Forensic Medicine, Jordan University Hospital, Amman, Jordan*

[8] *Department of Translational Medicine, Faculty of Medicine, Lund University, Malmö, Sweden*

[9] *Department of Electrical/Electronic and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria*

[10] *Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*

[11] *Hellenic Open University, School of Social Science, MPH Postgraduate Program, Public Health & Policies, Patra, Greece*

[12] *School of Electrical and Electronics Engineering, Lovely Professional University, Punjab, India,*

[13] *Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India*

ARTICLEINFO

Article History

Received 19 Mar 2025
Revised 7 May 2025
Accepted 1 Jul 2025
Published 22 Jul 2025

Keywords

Smart Logistics
Edge-Fog-Cloud Computing
Blockchain Technology
Federated Learning
Data Privacy

ABSTRACT

The rapid growth of smart logistics, driven by IoT devices and data-intensive applications, necessitates secure, scalable, and efficient computing frameworks. As the edge-fog-cloud (EFC) paradigm supports real-time data processing, it faces significant security threats and attacks, including privacy risks, data breaches, and unauthorized access. To address these security threats and attacks, blockchain and federated learning (FL) have gained popularity as potential solutions in EFC computing environments for smart logistics. This survey reviews the current landscape in EFC computing environments for smart logistics, highlighting the existing benefits and challenges identified in 134 research studies published between January 2023 and June 2025. The applications of blockchain and FL demonstrate their ability to enhance data security and privacy, improve real-time tracking and monitoring, and ensure inventory and supply chain optimization. Although these technologies offer promising solutions, challenges such as scalability issues, data quality, interoperability and standardization hinder their effective implementation. The survey suggests future research directions focused on developing advanced blockchain and FL, integrating emerging technologies, developing policies and regulations, fostering collaborative research, and ensuring cross-industry adoption and interoperability. Integrating blockchain and FL within the EFC model offers a transformative path toward building secure, intelligent, and resilient logistics systems.

1. INTRODUCTION

The globalization of supply chains and the rise of e-commerce have significantly transformed logistics operations, emphasizing the need for smarter, more efficient systems to handle the complexities of modern logistics networks [1]. Traditional logistics relies on manual processes and human intervention for inventory management and transportation, resulting in inefficiencies, delays, and reduced transparency. Digital technologies have revolutionized logistics and supply chain management, driving the shift toward smart logistics and enabling more efficient, responsive, and data-driven

*Corresponding author. Email: a.guma@muni.ac.ug

operations. Smart logistics uses advanced technologies such as IoT devices, global positioning system (GPS) tracking, radio-frequency identification (RFID), sensors, robotics and automation, blockchain, artificial intelligence (AI), and data analytics to optimize operations, enabling real-time tracking, predictive maintenance, automated decision-making, and the management of logistics processes, including warehousing, transportation, and delivery, which reduce costs and enhance service quality [2]. These systems enhance decision-making capabilities, reduce operational costs, and improve customer satisfaction by ensuring timely and accurate order fulfilment. Logistics and supply chains are essential to the global economy, with the industry valued at approximately 8.4 trillion euros in 2021 and projected to grow to over 13.7 trillion euros by 2027 [3]. According to reports and Insights' analysis, the global smart logistics market was valued at US$31.7 billion in 2023 and is projected to reach US$185.6 billion by 2032, growing at a compound annual growth rate (CAGR) of 21.7% during the forecast period. The rising demand for operational efficiency, cost reduction in supply chain management, and the need for end-to-end visibility and transparency are driving the adoption of smart logistics solutions.

The adoption of EFC computing has emerged as a crucial technological framework for supporting the dynamic and real-time nature of smart logistics. Edge computing brings data processing closer to the source of data generation, reducing latency and improving response times. It reduces the time required to process data, making it ideal for applications where low latency is crucial, such as autonomous vehicles, industrial IoT sensors, and wearable devices, or where cloud interactions are unnecessary. Its speed and efficiency benefits appeal to both the consumer and industrial sectors. Fog computing is a distributed model that enhances edge computing by adding a layer of infrastructure between edge devices and the cloud. The fog layer offers additional computing resources and services to support edge devices, enhancing scalability and operational efficiency. Autonomous vehicles and smart cities are prime examples of fog computing applications. Autonomous vehicles utilize sensors and cameras to gather data and make real-time navigation decisions, whereas smart cities leverage a network of sensors and devices to optimize services and infrastructure [4][5]. Cloud computing relies on centralized data centers located globally, introducing latency due to data transmission to and from the cloud. It requires high-bandwidth connectivity and leverages the powerful processing capabilities of data centers, offering high scalability for on-demand computational and storage resources. This approach is ideal for applications that require substantial computational power and storage, such as big data analytics, machine learning, and AI [6].

Despite the robust computational power and data storage capabilities offered by EFC architectures in smart logistics, it faces several security threats, attacks, and vulnerabilities, including data privacy violations, data breaches, unauthorized access, distributed denial-of-service (DDoS) attacks, man-in-the-middle (MitM) attacks, malware, ransomware-as-a-service (RaaS), supply chain attacks, insider threats, phishing attacks, quantum computing threats, malicious code injection, eavesdropping attacks, spoofing attacks, physical security breaches, IoT device vulnerabilities, and firmware and software vulnerabilities [6-18]. These security threats, attacks, and vulnerabilities have resulted in supply chain disruptions, data breaches, and the loss of confidential information, as well as risks to IoT device compromise, cloud infrastructure, and data integrity. These threats have led to significant consequences, including supply chain disruptions, data breaches, loss of confidential information, operational downtime, compromised IoT devices, cloud infrastructure compromise, data integrity loss, financial losses, erosion of stakeholder trust, regulatory and legal consequences, phishing and insider threat exploitation, increased attack surface, reputation damage, delayed deliveries and routing errors, and increased mitigation and recovery costs.

This survey aims to address pressing security threats and challenges by exploring the synergistic integration of blockchain and FL within the EFC computing framework for smart logistics. Blockchain technology offers decentralized and secure data management, ensuring data integrity, traceability, and stakeholder trust [19]. Whereas FL allows decentralized ML model training while maintaining the privacy of sensitive data, it is an ideal solution for collaborative intelligence in smart logistics networks [20]. Blockchain eliminates the need for a central authority, reducing single points of failure and enhancing system robustness [19][21]. Blockchain in data management systems provides a tamper-proof environment, ensuring that data remain unaltered and traceable. This is particularly beneficial in scenarios where data authenticity and trust are paramount. It also uses consensus mechanisms, cryptography, and smart contracts to facilitate secure transactions without the need for a central authority. With features such as anonymity, tamper resistance, and decentralization, blockchain is widely applied in areas such as in-vehicle networks, the industrial IoT, and medical networks [19-21]. In FL, the blockchain's distributed trust model enables secure communication between untrusted participants without a central authority, addressing challenges such as malicious actors. Blockchain-based FL leverages smart contracts to defend against poisoning attacks and ensure secure updates [19]. Federated learning addresses privacy concerns by ensuring that sensitive data remain on local devices, reducing the risk of data breaches associated with centralized data storage. FL is especially advantageous in environments where data privacy regulations are stringent, as it allows for the utilization of data insights without compromising individual privacy [19][20]. Integrating blockchain with FL in smart logistics offers a robust solution to data security, privacy, and scalability challenges. Blockchain ensures the secure aggregation and verification of local model updates, providing an immutable and transparent framework that enhances the trustworthiness of the FL process [19][22]. In a blockchain-based FL system, training nodes download an initialized model, perform local training, and upload updates as blockchain transactions. Miner nodes verify these transactions, append them to the blockchain, and distribute the updated global model for the next training round. This decentralized approach ensures secure communication and reliable model

aggregation [19][22]. While computational overhead remains a concern, the convergence of blockchain and FL in EFC computing environments for smart logistics presents significant opportunities [20][21][23] by enabling real-time decision-making, preserving data privacy in machine learning, and supporting the scalability of distributed logistics applications. By leveraging these technologies, the framework strengthens data security and privacy, enables real-time tracking and monitoring, optimizes inventory and supply chain operations, and supports autonomous logistics functions. It also facilitates fraud detection, risk management, smart contract automation, and collaborative data sharing for joint learning and informed decision-making. Furthermore, the framework enhances collaborative fleet management, increases supply chain transparency and provenance, supports autonomous delivery systems, and enables the tracking of sustainability metrics and carbon footprints. By incorporating this approach, blockchain and FL within EFC computing environments address key security threats and challenges in smart logistics, offering a robust solution for modern logistics management.

This survey explores the integration of blockchain and FL within EFC computing environments for smart logistics, focusing on current applications, challenges, and future research directions. By examining these emerging technologies, this review aims to provide a comprehensive understanding of their potential impact on smart logistics, contributing to the design of secure, scalable, and intelligent supply chain systems.

The contributions of this review include the following:

- To explore the foundations and theoretical background, an overview of smart logistics, EFC computing for smart logistics, the benefits of EFC computing in smart logistics, and the security threats and attacks faced by EFC computing in smart logistics is needed.
- To describe the concepts of blockchain technology and FL.
- To explain the convergence of blockchain technology, FL, and EFC computing in smart logistics.
- To describe the integration of blockchain and FL in EFC computing environments for smart logistics.
- To examine the applications of blockchain and FL within EFC computing environments in smart logistics.
- To explore case studies and practical implementations of blockchain and FL in EFC computing environments for smart logistics.
- To identify key challenges and limitations associated with integrating blockchain and FL within the EFC computing environment for logistics operations.
- To provide insights into future research directions.

This survey bridges the gap between theoretical potential and practical deployment by establishing a foundation for resilient, secure, and intelligent logistics ecosystems. This demonstrates how the combined strengths of blockchain and FL, when integrated into EFC infrastructures, can enable decentralized, privacy-preserving, and trustworthy operations in smart logistics environments.

This review is structured into multiple sections. This section begins with an introduction, followed by an outline of the materials and methods in Section 2. Section 3 discusses foundational theories and background, while Section 4 explores the integration of blockchain and FL within EFC environments. Section 5 highlights applications in smart logistics, followed by case studies and practical implementations in Section 6. Section 7 addresses key challenges and limitations, and Section 8 identifies future research directions. The review concludes in Section 9.

2. MATERIALS AND METHODS

Researchers have comprehensively reviewed the literature on leveraging blockchain and FL in edge computing environments for smart logistics. The primary objective was to identify, evaluate, and synthesize key research articles published between January 1, 2023, and May 2025, with a focus on integrating blockchain technology and FL within EFC for smart logistics. To ensure thorough field coverage, the researchers utilized targeted keywords to gather relevant literature from several scientific databases, including the ACM Digital Library, Frontiers, Wiley Online Library, PLoS ONE, IGI Global, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, Emerald Insight, and Google Scholar.

Specific search terms and Boolean operators were employed to tailor the searches for each database, such as "Blockchain" OR "Distributed Ledger" AND "Federated Learning" OR "Collaborative Learning" AND "Edge Computing" OR "Fog Computing" AND "Smart Logistics" OR "Intelligent Transportation" OR "Supply Chain". Boolean operators were utilized to refine the search results across various subdomains of “learning blockchain and FL in EFC computing environments for smart logistics,” ensuring the inclusion of only pertinent materials. Keywords were further tailored to align with the specific search functionalities of each database.

The authors independently gathered relevant research papers from the selected databases on the basis of predefined criteria, including (1) the title, authors, and publication year; (2) objectives and research questions; (3) study design; (4) blockchain technology; (5) FL in EFC computing; (6) blockchain-based FL in EFC computing environments for smart logistics; (7) applications in smart logistics; (8) case studies and practical implementations; (9) challenges and limitations; (10) future trends and research directions; and (11) conclusions. The collected information was systematically organized to ensure consistency and accuracy.

Relevant review materials were selected on the basis of defined inclusion and exclusion criteria, facilitating careful literature screening. These criteria ensure that the chosen materials are of high quality, directly applicable, and relevant to blockchain-based FL in EFC computing environments for smart logistics, as detailed in Table 1.

TABLE I. SUMMARY OF THE INCLUSION AND EXCLUSION CRITERIA FOR CHOOSING RELEVANT RESEARCH PAPERS.

S/No		Inclusion Criteria	Exclusion Criteria
1	Relevance to the topic	Studies discussing Blockchain and FL in EFC computing environments for smart logistics.	Studies that do not involve Blockchain or FL in smart logistics.
2	Publication type	Peer-reviewed journal articles, conference papers, books, and book chapters.	Non-peer-reviewed articles, opinion pieces, or blogs.
3	Time frame	Publications from January 2023 to May 2025, capturing the latest advancements.	Publications before 2023.
4	Methodology	Empirical studies, simulations, theoretical models, case studies, and frameworks.	Studies that lack robust methodology, experiments, or analysis.
5	Language	Publications in English.	Publications not in English.
6	Quality and depth	High-quality research studies with transparent methodology and significant theoretical or empirical contributions.	Low-quality studies with insufficient detail, unclear methodologies, or a lack of scientific rigor.

The initial database search results were carefully screened to identify and remove duplicates. The remaining research papers underwent a preliminary review, where titles and abstracts were assessed for relevance. Papers considered suitable were then subjected to a detailed full-text review to confirm their eligibility on the basis of predefined inclusion and exclusion criteria. This screening and selection process was carried out independently by five reviewers. A test–retest approach was implemented to reduce potential biases when applying exclusion criteria. Randomly selected papers were re-evaluated multiple times to ensure consistency and accuracy in the selection process. Ultimately, 134 relevant publications were included in the review, comprising 5 from the ACM Digital Library, 1 from Frontiers, 5 from the Wiley Online Library, 1 from PLoS ONE, 1 from IGI Global, 11 from Springer, 19 from ScienceDirect, 26 from MDPI, 16 from the IEEE Xplore Digital Library, 1 from Emerald Insight, and 48 from Google Scholar. The selected studies were systematically analysed, evaluated, and categorized on the basis of their relevance to leveraging blockchain and FL within EFC computing environments for smart logistics. The categorization of these research papers is shown in Fig. 1.

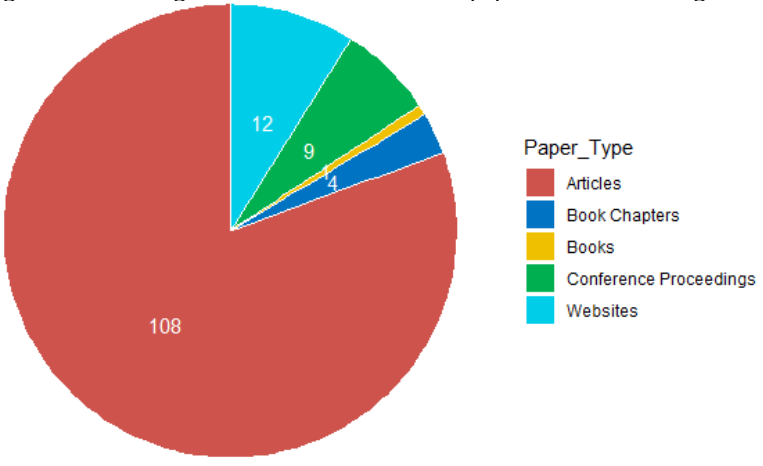

Fig. 1. The categories of research papers selected for the study

Fig. 2 shows the digital databases used to retrieve the selected research papers for the survey.

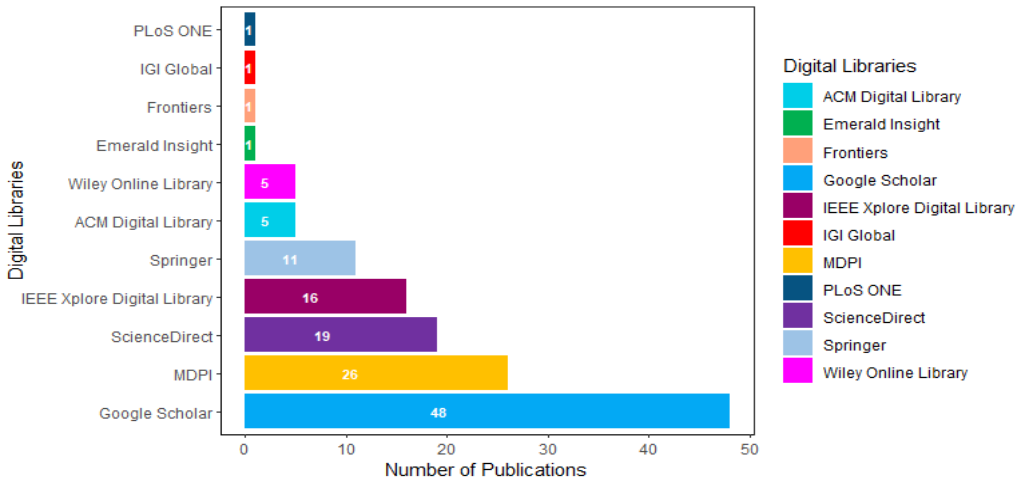

Fig. 2. Depicts the digital databases used to retrieve the selected research papers for the survey.

Fig. 3 illustrates the distribution of research paper sources across digital libraries.

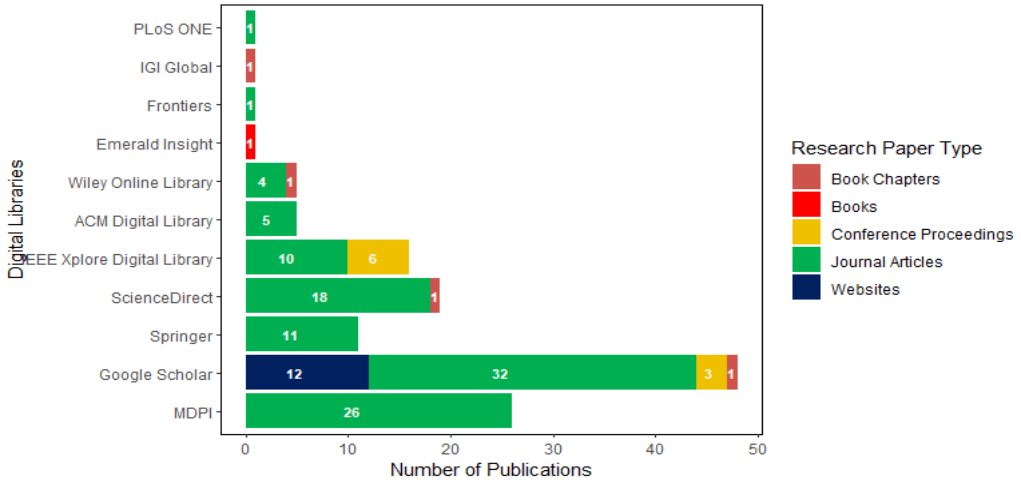

Fig. 3. Depicts the distribution of research paper sources based on digital libraries.

Fig. 4 illustrates the distribution of papers selected by digital libraries, categorized by the year of publication.

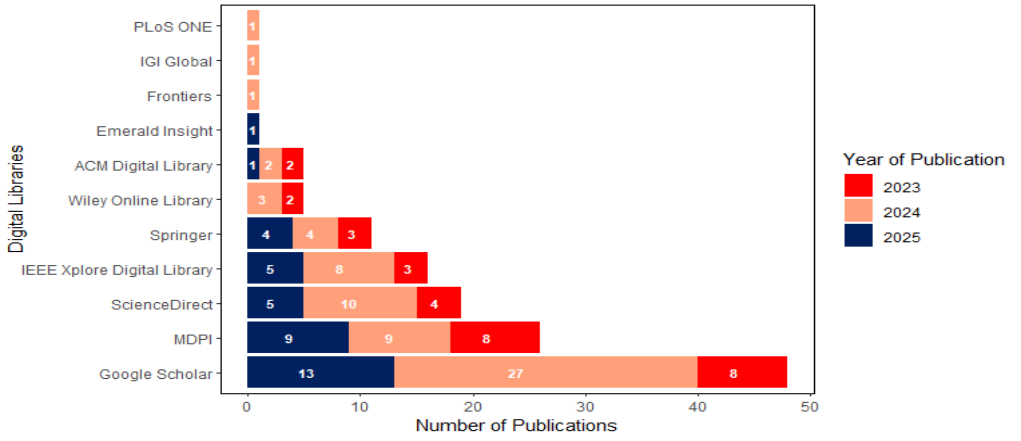

Fig. 4. Distribution of papers selected by digital libraries on the basis of the year of publication.

The researchers systematically extracted data from each selected study to collect relevant information for thematic synthesis. Data fields included publication details, study focus, technologies (blockchain, FL, and EFC computing), applications (specifically leveraging these technologies for smart logistics), and methodologies.

Thematic analysis was conducted to categorize the studies on the basis of application areas and domains within smart logistics. Additionally, the research was classified according to technological approaches, highlighting the blockchain and FL environments within EFC systems. Qualitative synthesis and thematic analysis methods were used to analyse the data. To validate the review findings, subject matter experts were consulted, the results were cross-referenced with literature, and the robustness of the conclusions was critically assessed. Each study was evaluated for quality on the basis of its methodological rigor, the reliability and validity of its findings, and its relevance to blockchain and FL in EFC computing for smart logistics. Since the review focused on analysing secondary literature, no primary data were collected, eliminating the need for ethical approval. However, ethical standards were maintained by properly citing sources and avoiding plagiarism. A subset of studies emphasizing methodologies and performance measures was closely examined to explore the synergistic potential of blockchain and FL in EFC computing for smart logistics. The factors considered during the evaluation included the technologies applied, their integration with logistics operations, the relevance of the insights provided, and the robustness of the methodologies used.

Despite its comprehensive approach, the study faced certain limitations. Rapid advancements in blockchain and FL within EFC environments meant that some recent developments might have been overlooked. Only studies published in English and accessible through major scientific databases were included, potentially excluding relevant research published in languages other than English or niche outlets. The lack of quantitative analysis or empirical data may weaken the review's robustness, as qualitative evaluations can only partially support the claims. The review may overlook practical challenges associated with real-world implementation by emphasizing theoretical applications. Additionally, as smart logistics initiatives evolve, emerging technological approaches and challenges may impact the relevance and applicability of this analysis.

3. FOUNDATIONS AND THEORETICAL BACKGROUND

3.1. Overview of Smart Logistics

Smart logistics, also referred to as "intelligent logistics" or "logistics 4.0," originates from IBM's concept of the "intelligent logistics system." Although no universally accepted definition exists, it is widely understood to involve the application of advanced technologies and data-driven strategies to optimize logistics planning, management, and control [24]. Smart logistics leverages IoT, AI, cloud computing, and big data analytics to create a more efficient, responsive, and automated supply chain ecosystem. The global smart logistics market, valued at US$250 billion in 2025, is projected to grow at a 15% compound annual growth rate (CAGR), reaching US$750 billion by 2033. This growth is driven by increasing demand for efficient supply chains, fueled by the adoption of the IoT, advanced analytics, and automation [25]. Key sectors, including manufacturing, energy, and food and beverage, are driving demands for optimized logistics solutions to increase speed and reliability.

Smart logistics relies on several core components that enhance efficiency, visibility, and decision-making across the supply chain. IoT devices—such as GPS trackers, RFID tags, and environmental sensors—deliver real-time data on the location, condition, and status of goods, enabling continuous monitoring. AI and machine learning algorithms analyse large datasets to predict demand, optimize routing, automate decisions, detect anomalies, and continually improve over time through exposure to both historical and real-time data. Big data and predictive analytics identify trends, forecast disruptions, and support proactive responses to traffic congestion or inventory shortages. Cloud computing provides a scalable infrastructure for storing, sharing, and analysing logistics data, facilitating collaboration and real-time coordination across multiple sites. Autonomous and connected systems, including drones, self-driving vehicles, and delivery robots, reduce dependence on human labor and increase delivery speed and accuracy. Moreover, blockchain technology enhances transparency and security by creating immutable records and enabling smart contracts, which prove especially valuable in international trade and cold-chain logistics.

Smart logistics enhances operational efficiency through several key functions and applications. It enables real-time inventory management by monitoring stock levels, automating reordering, and optimizing warehouse storage with the aid of robotics and AI systems. Dynamic routing algorithms analyse traffic, weather, and delivery schedules to identify the most efficient transportation routes, minimizing fuel consumption and delivery times. Businesses and customers can track shipments in real time, receiving timely updates on delays or incidents. Smart logistics also improves demand forecasting by analysing historical sales data, seasonal patterns, and market trends to inform procurement and production decisions. Automated warehouses utilize robots and automated guided vehicles (AGVs) to handle picking, packing, and shipping tasks with minimal human intervention, thereby reducing errors and enhancing efficiency. Smart logistics enhances the customer experience by providing accurate delivery estimates, flexible delivery options, and proactive communication. Smart logistics offers numerous benefits by improving operational efficiency through automation and real-time data, which reduces delays,

lowers costs, and increases throughput. It increases visibility and transparency across the supply chain, fostering greater trust and accountability. By optimizing routes and resource usage, smart logistics supports sustainability through reduced carbon emissions.

Additionally, real-time monitoring and predictive analytics strengthen risk management by identifying and addressing potential disruptions early. Finally, these systems scale effectively, handling growing volumes and complexity without requiring a proportional increase in resources [7-9]. Fig. 5 illustrates the concept of smart logistics.

Fig. 5. Conceptual illustration of smart logistics.

3.2. Edge-Fog-Cloud Computing for Smart Logistics

Edge-fog-cloud computing refers to a hierarchical computing architecture that integrates the distinct capabilities of edge, fog, and cloud computing. This architecture optimizes resource utilization and data processing efficiency in distributed environments, enabling real-time analytics and improved decision-making. EFC computing has gained significant attention in smart logistics systems because of its ability to handle the massive amounts of data generated by IoT devices, sensors, and connected systems [6][26]. The layered architecture of EFC computing in smart logistics includes the following layers.

3.2.1. Data collection layer (perception layer)

This foundational layer is responsible for sensing and collecting real-time data from the logistics environment. It includes RFID tags, GPS trackers, barcode scanners, cameras, temperature and humidity sensors, and IoT-enabled vehicles or containers. It is located at the network edge and enables low-latency data acquisition and preprocessing, ensuring efficient transmission to the fog and cloud layers for further analysis and processing. It detects and records data related to package location, environmental conditions, vehicle telemetry, and warehouse operations, providing accurate, real-time data for downstream processing [6][26].

3.2.2. Edge computing layer

This layer is closest to the data sources and performs initial data processing to reduce latency and bandwidth usage. It includes embedded systems, mobile devices, gateways, and edge routers, which filter, aggregate, and perform lightweight analytics on data (e.g., anomaly detection real-time alerts), reducing data transmission to centralized systems. Edge computing leverages local processing power to minimize latency and facilitate real-time data processing for smart logistics applications. Reducing dependence on cloud transmission enhances efficiency, but high bandwidth is required for data exchange when needed. It offers low latency and improved responsiveness, such as rerouting delivery vehicles on the basis of traffic data [6][26].

3.2.3. Fog computing layer

The fog computing layer acts as a mediator between edge devices and cloud services, providing additional computing resources closer to the data sources. It offers intermediate data aggregation, processing, and storage. This includes devices such as local servers, network switches, routers with computing capabilities, and micro data centers at logistics hubs. Fog computing employs a hierarchical structure in which edge devices connect directly to fog nodes, thereby bypassing the cloud and extending cloud capabilities to the network edge. It balances processing between the edge and the cloud, reducing

bandwidth needs but introducing some latency. The primary functions are intermediate processing and storage, supporting distributed analytics and decision-making, and coordinating multiple edge nodes. It is primarily used in processing fleet-wide logistics data for regional optimization without requiring all data to be sent to the cloud. With more powerful nodes than edge devices, it supports applications requiring greater processing power in smart logistics [6].

3.2.4. Cloud computing layer

This is the central hub for large-scale data storage, complex analytics, and global decision-making, enabling high scalability for big data analytics, AI, and machine learning applications. It consists of Cloud data centers (e.g., AWS, Azure, Google Cloud), and its primary function is to perform deep analytics via AI/machine learning models, centralized control and orchestration, and historical data archiving. Although it requires high bandwidth and introduces latency due to data transmission, it ensures advanced security. Unlike fog computing, which processes data closer to edge devices, cloud computing supports large-scale, on-demand resource provisioning, albeit less suitable for real-time applications. It is mainly used in predictive modelling for demand forecasting, route optimization, and global supply chain coordination [15].

3.2.5. Infrastructure layer (IaaS)

The IaaS layer provides the foundational virtualized hardware resources that support the cloud and fog layers, including virtual machines, storage, and network resources. There is a public (e.g., AWS EC2, Google Compute Engine) or private cloud infrastructure that offers scalability for storage and computation, as well as flexible deployment for various logistics applications. IaaS enables organizations to scale resources according to demand without significant capital investment in smart logistics, facilitating flexibility and cost efficiency [15].

3.2.6. Platform layer (PaaS)

The PaaS layer provides development tools and frameworks for building, deploying, and managing logistics applications. It consists of APIs, container platforms (e.g., Kubernetes), and development environments, among other components. These tools provide abstracted hardware complexities, enable scalable app development and integration, and support microservices for logistics operations, such as warehouse automation modules. In logistics, PaaS facilitates the creation of custom applications for tasks such as route optimization, inventory management, and real-time tracking without the complexity of managing the underlying hardware and software layers [15].

3.2.7. Application as a layer (SaaS)

The Software as a Service (SaaS) layer provides host end-user logistics applications that leverage processed data for business operations, such as fleet management systems, warehouse management systems (WMS), transportation management systems (TMS), and customer tracking and notification apps. These applications interface with stakeholders, including drivers, warehouse staff, and managers, providing decision support, inventory tracking, route optimization, fleet management, reporting, and visualization [15].

3.2.8. Data management and storage

This transversal layer ensures efficient data handling across the architecture, facilitating data ingestion, transformation, and federation across EFC, as well as metadata tagging and data lineage tracking for logistics data. It supports data lakes and structured warehouses, utilizing tools such as Apache Kafka, Hadoop, and NoSQL/SQL databases [15].

3.2.9. Security layer

The security layer ensures data integrity, confidentiality, and access control throughout the architecture. It features components such as encryption protocols (transport layer security, advanced encryption standards), authentication and authorization (OAuth, biometrics), and secure communication (virtual private networks, firewalls). This is used to prevent tampering with shipment data, ensure only authorized access to sensitive logistics information, and ensure safe transactions across the supply chain.

3.2.10. Management and monitoring tools

These tools facilitate the orchestration of all components, real-time tracking, and performance monitoring. It is used in health monitoring of devices and applications, resource usage tracking, and failure detection and alerting. These tools leverage various technologies, including Prometheus, Grafana, ELK stack, AWS CloudWatch, and others. Logistics enable real-time monitoring of operations, performance metrics, and resource utilization, facilitating proactive management and quick response to issues [15].

3.2.11. Journal analysis layer

This layer supports strategic decision-making and provides academic and business insights through in-depth analytics and reporting. It is used for logging, auditing, and compliance tracking in smart logistics. The journal analysis layer conducts

longitudinal studies using archived logistics data; facilitates knowledge discovery, trend analysis, and evaluation of key performance indicators; and integrates with business intelligence tools for visual analytics. It maintains immutable records of all system activities and transactions, supporting anomaly detection, security audits, and performance analysis by examining historical logs. Data scientists, logistics analysts, and academic researchers use it [15]. Fig. 6 illustrates the layered architecture of EFC computing in smart logistics.

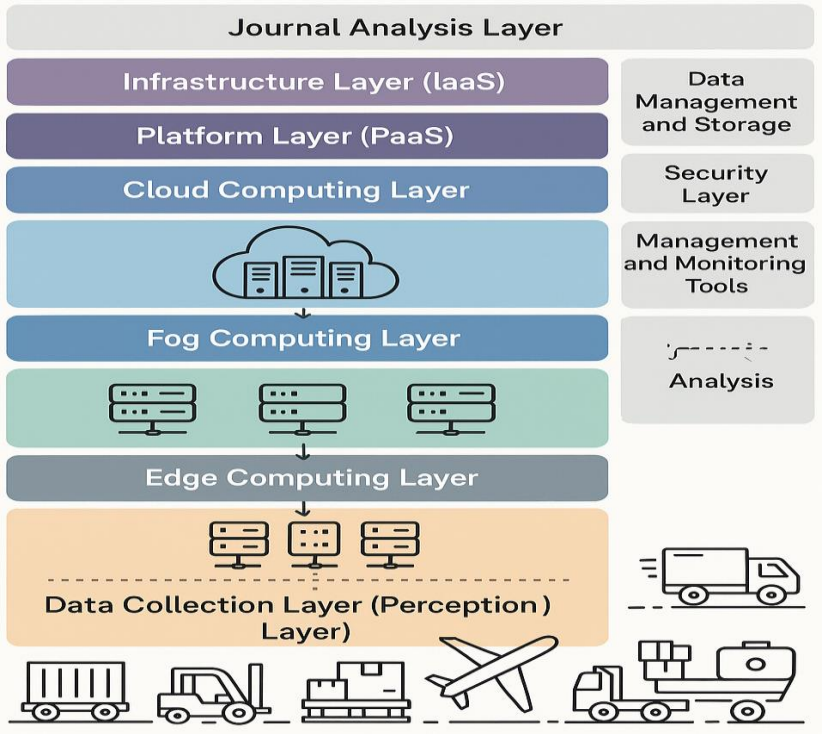

Fig. 6. Illustrates the layered architecture of EFC computing in smart logistics.

3.3. Benefits of EFC Computing in Smart Logistics

The EFC computing model transforms smart logistics by enabling real-time data processing, enhanced efficiency, and secure data management. Using a decentralized architecture, EFC optimizes smart logistics operations by distributing workloads across edge devices, fog nodes, and cloud systems, offering key benefits in logistics operations. Table 2 summarizes the benefits of EFC computing in smart logistics.

TABLE II. SUMMARY OF THE KEY BENEFITS OF EFC COMPUTING IN SMART LOGISTICS.

S/No	Benefits	Description	References
1	Latency reduction	Low-latency processing at the edge enables real-time decision-making, thereby reducing transmission delays for applications such as autonomous vehicles and industrial automation. Specialized hardware, such as Field-Programmable Gate Arrays (FPGAs) and Graphics Processing Units (GPUs), enhances computational speed, minimizing round-trip latency for logistics operations like inventory tracking and route optimization.	[27]
2	Distributed processing	The layered architecture of EFC computing enables distributed data processing, optimizes resource utilization, and prevents common bottlenecks associated with centralized processing.	[6][27]
3	Network bandwidth optimization	Local edge and fog computing reduce the volume of data sent to the cloud, improving network efficiency and bandwidth utilization. By transmitting only essential processed insights, businesses lower network dependency and costs.	[6][27]
4	Enhanced reliability	EFC computing enhances fault tolerance by distributing processing across multiple layers. Edge devices ensure continued operation even with limited cloud connectivity, maintaining decision-making capabilities in unstable network conditions.	[27]
5	Scalability	The hierarchical design of EFC computing enables the seamless expansion of logistics systems, allowing for the integration of additional devices and sensors without compromising performance. Edge, fog, and cloud layers offer varying scalability levels, ranging from localized expansion to large-scale cloud storage and computing.	[27]

3.4. Security threats, attacks, and vulnerabilities faced by EFC computing in smart logistics

Integrating edge, fog, and cloud computing architectures forms the backbone of modern smart logistics systems by enabling real-time data processing, greater scalability, and improved operational efficiency through the distributed execution of computational tasks across edge devices, fog nodes, and centralized cloud platforms. However, this heterogeneous and decentralized setup significantly expands the attack surface, exposing these systems to a wide range of security threats, attacks, and vulnerabilities, including the following.

3.4.1. Data privacy violation

Data privacy violations present significant challenges for smart logistics systems operating within EFC computing architectures. While these layered architectures enhance efficiency and responsiveness, they complicate data handling and increase the risk of privacy breaches. Key concerns include an expanded attack surface resulting from the proliferation of IoT devices, such as GPS trackers, RFID readers, and environmental sensors, which serve as potential entry points for cyberattacks. Inconsistent security protocols across edge, fog, and cloud layers further exacerbate vulnerabilities, as edge devices often lack the robust protection of cloud systems. Data transmission between these layers remains susceptible to interception, particularly if encryption is weak or absent, allowing MitM attacks that compromise data confidentiality and integrity. Navigating regulatory compliance, particularly with laws such as the GDPR, becomes increasingly complex as data cross multiple jurisdictions with varying legal requirements. Real-world incidents underscore these risks: in 2024, attackers exploited vulnerabilities in edge tracking devices, gaining unauthorized access to customer delivery schedules and personal information. In another case, outdated firmware on fog nodes in a smart warehouse allows attackers to infiltrate the system and access sensitive inventory data, emphasizing the need for consistent security updates and patch management across all layers [6][11][12][15][26].

3.4.2. Data breach

Data breaches in EFC computing architectures pose critical risks to smart logistics systems, which depend on real-time data processing and interconnected devices. In May 2023, attackers from the CL0P ransomware group exploited a zero-day vulnerability in Progress Software's MOVEit Transfer, a widely used managed file transfer solution. This vulnerability enabled SQL injection attacks that compromised over 2,700 organizations and exposed the personal data of approximately 93.3 million individuals, including entities in logistics-related sectors such as transportation and government agencies. In 2024, cybercriminals breached Snowflake Inc., a cloud-based data warehousing company, by exploiting exposed credentials to access customer data, affecting companies such as Ticketmaster, Advance Auto Parts, and Santander Bank. The incident underscored the vulnerabilities of centralized cloud storage and the necessity of securing authentication mechanisms. Dell Technologies also suffered multiple breaches in 2024, including a hacker offering for the sale of 49 million customer records spanning purchases from 2017--2024. These incidents highlight significant weaknesses in supply chain data management and internal security protocols. Integrating edge, fog, and cloud computing in smart logistics introduces key security challenges: (i) a distributed attack surface that complicates endpoint monitoring and protection; (ii) limited computational resources at the edge and fog levels that hinder robust security implementation; (iii) vulnerabilities in data transmission between layers if encryption is inadequate; and (iv) security gaps stemming from reliance on third-party services that may lack stringent safeguards [6][12][15][16][26].

3.4.3. Unauthorized access

Unauthorized access to management interfaces in EFC computing environments presents significant security risks, especially in smart logistics systems that rely on real-time data processing and decentralized architectures. These risks stem from the distributed and heterogeneous nature of such systems, as well as inconsistent security measures across different layers. Attackers who exploit weak authentication mechanisms—often default or easily guessable credentials—can gain control over management interfaces, enabling them to alter routing algorithms, delay deliveries, or disrupt operations. Inadequate access controls and unencrypted communication channels expose these systems to privilege escalation, data interception, and manipulation. Outdated firmware or unpatched software increases vulnerability to exploitation. In logistics, these breaches can compromise sensitive data, disrupt supply chains, and lead to substantial financial losses. For example, attackers could modify warehouse inventory data through fog node interfaces, leading to operational inefficiencies or the exfiltration of shipment and customer information, which could result in competitive or regulatory consequences. They may also shut down critical services, such as real-time tracking or automated sorting, resulting in substantial downtime and halting logistics operations [6][11][12][15][26].

3.4.4. Distributed denial-of-service (DDoS) attacks

DDoS attacks pose a serious threat to EFC computing architectures, particularly in smart logistics systems. Integrating IoT devices in logistics has expanded the attack surface, increasing the vulnerability of these systems. Attackers exploit weaknesses in IoT devices to launch large-scale, botnet-driven DDoS attacks that target edge devices, fog nodes, and cloud services. These attacks overwhelm system resources, disrupt real-time tracking, delay shipments, and impair coordination

across the logistics network. In 2023, IoT-based DDoS attacks increased by 68% year over year, driven primarily by botnets such as Mirai variants, which now utilize residential IP addresses and cloud instances to amplify their impact. Some of these botnets can generate over 8.5 million requests per second via devices such as smart TVs and edge routers. For example, Cloudflare reported a record-breaking HTTP DDoS attack in early 2023, peaking at 71 million requests per second. The pro-Russian hacker group NoName057(16) also targeted the logistics and transportation sectors across Europe and North America. These layers are particularly susceptible, given the decentralized nature of the edge and fog nodes and their limited resources. DDoS attacks severely disrupt the real-time data processing and communication required in smart logistics, leading to operational delays, resource exhaustion, and potential security breaches [6][10][12][15][26].

3.4.5. Man-in-the-middle (MitM) attacks

MitM attacks pose significant threats to EFC computing architectures, particularly in smart logistics systems where maintaining real-time data integrity and confidentiality is critical. These attacks intercept device communications by exploiting vulnerabilities in decentralized, resource-constrained environments. Adversaries can intercept, alter, or reroute data as they move from edge devices (e.g., RFID scanners, GPS trackers) to fog nodes (e.g., local gateways) and then to centralized cloud platforms for processing. Attackers may target various points along this path, including intercepting poorly secured edge-to-fog communications, compromising fog nodes by impersonating legitimate gateways or tampering with data during fog-to-cloud transmission if robust security protocols are not in place. Lightweight security measures are often deployed in fog environments because limited resources may not withstand sophisticated attacks, allowing unauthorized access to shipment data. For example, intercepting data between IoT sensors and fog nodes can compromise cargo details, whereas rogue gateways can manipulate or redirect information. Moreover, the dynamic nature of fog networks complicates session management, enabling attackers to exploit session resumption algorithms and hijack sessions. Similar incidents in smart grid environments—closely related to logistics systems—have demonstrated that MitM attacks can inject false data, disrupt operations, and lead to real-world consequences [12].

3.4.6. Malware

Integrating edge, fog, and cloud computing in smart logistics has improved operational efficiency; however, it has also introduced complex cybersecurity threats, such as malware. Malware can infiltrate these systems through compromised devices or software updates, disrupting supply chains, compromising sensitive data, and causing financial losses. Edge devices—such as IoT sensors and mobile units—often serve as the first point of contact and remain vulnerable because of limited computational resources and weak security measures. The rise of IoT devices has enabled botnets such as Mozi and Gafgyt to exploit vulnerabilities in routers and cameras, launching DDoS attacks that disrupt logistics operations. In 2025, the Lynx ransomware attack on Allied Telesis, a networking hardware provider, encrypted approximately 800 GB of data, demonstrating the severe impact such incidents can have on logistics networks. Fog computing, which provides localized processing between edge and cloud layers, faces targeted threats. Attackers can deploy malicious or rogue fog nodes that impersonate legitimate devices to intercept, manipulate, or disrupt data flows. Ephemeral secret leakage attacks exploit temporary cryptographic keys to access and decrypt sensitive logistics data. At the cloud level, attackers use Trojan horse malware to infiltrate systems and alter or halt operations, while Ransomware-as-a-Service (RaaS) has lowered the barrier to deploying ransomware. The surge in ransomware attacks—up to 95% in 2024—underscores the cloud's appeal as a high-value target for cybercriminals [12].

3.4.7. Ransomware-as-a-Service (RaaS)

RaaS poses a significant threat to smart logistics systems operating within EFC computing architectures. These layered and decentralized systems present a broad attack surface that RaaS actors exploit vigorously. Operating on a subscription-based model, RaaS enables cybercriminals, including those with limited technical expertise, to lease ransomware tools and infrastructure, democratizing the launch of complex attacks. Threat actors frequently exploit vulnerabilities such as credential theft, misconfigurations, and lateral network movement to deploy ransomware that encrypts critical logistics data, halting operations and demanding ransoms. Groups such as LockBit, which resurfaced in 2024 with enhanced tactics after law enforcement crackdowns, have targeted sectors such as logistics by exploiting VMware ESXi flaws and leveraging insider threats. Similarly, fog ransomware, which emerged in April 2024, has rapidly targeted the logistics, education, and manufacturing sectors through compromised VPN credentials and swift double extortion attacks. Black Basta has escalated attacks on industrial systems, notably disrupting ABB in 2023 via Windows's active directory vulnerabilities. These incidents highlight how integrating EFC systems while enhancing efficiency also introduces vulnerabilities, such as supply chain disruptions, data exfiltration, and operational downtime, which RaaS operators continue to exploit [12].

3.4.8. Supply chain attacks

Supply chain attacks in EFC computing environments pose serious threats to smart logistics systems by exploiting vulnerabilities across interconnected layers, including edge devices, fog nodes, and the cloud infrastructure. These attacks often begin with the least secure components and propagate through the system, disrupting operations, compromising data

integrity, and causing significant financial losses. In logistics, for example, a compromised software update from a vendor can inject malicious code into the system. Analysing the power consumption patterns of edge devices can also reveal sensitive operational data. While enabling efficient data processing and decision-making, the EFC model remains susceptible to such threats. High-profile incidents underscore these risks: in March 2023, attackers compromised the 3CX Desktop App by infiltrating its built environment and distributing a Trojanized version through official update channels; in October 2023, attackers breached Okta's customer support system by stealing an employee's credentials, gaining access to sensitive customer data and affecting clients such as 1 Password and Cloudflare. These incidents reveal how supply chain attacks can disrupt operations, corrupt or steal critical data, and expose systems to unauthorized access, ultimately eroding trust and violating compliance standards in smart logistics [6][15][26].

3.4.9. Insider threats

Insider threats in EFC computing architectures pose significant challenges to intelligent logistics systems, where data are exchanged across distributed environments. These threats arise from individuals within organizations who exploit legitimate access to compromise data integrity, disrupt operations, or exfiltrate sensitive information. The integration of edge, fog, and cloud computing enhances real-time data processing and decision-making but also broadens the attack surface, increasing vulnerability to insider threats. Insiders typically fall into three categories: malicious insiders who intentionally misuse access for personal gain or to harm the organization; negligent insiders who unintentionally compromise security through careless actions, such as system misconfigurations or falling victim to phishing attacks; and compromised insiders whose stolen credentials are used by external actors. For example, an insider might leak shipment data, resulting in stolen or operational losses. Employees with access to physical servers, particularly those working for cloud service providers, pose significant risks if they engage in unauthorized or malicious activities. In a 2023 case, a logistics company discovered an employee selling confidential customer data to competitors, resulting in severe reputational damage and legal repercussions [6][15][17][26].

3.4.10. Phishing attacks

Phishing attacks have grown increasingly sophisticated, threatening EFC computing architectures in smart logistics systems by exploiting human and technological vulnerabilities across all layers. Employees at the edge often receive spear-phishing emails impersonating trusted partners or clone phishing messages with malicious links, which can lead to credential theft and unauthorized access. This was evident in a case where attackers posing as a CEO fraudulently obtained US$500,000. At the fog layer, attackers target rogue fog nodes masquerading as legitimate nodes to intercept or manipulate data and execute MitM attacks that compromise communications between edge devices and the cloud. These compromised fog nodes can process or redirect sensitive logistics data, causing confidentiality and integrity breaches. Moreover, attackers exploit the cloud layer by phishing for user credentials to access sensitive data and deploying AI-driven phishing campaigns that craft compelling messages.

3.4.11. Quantum computing threats

Quantum computing poses significant security threats to the EFC architectures that are essential for smart logistics. As quantum capabilities evolve, they render traditional cryptographic methods obsolete, forcing a comprehensive overhaul of security measures across these distributed systems. Quantum algorithms, such as Shor's algorithm, can efficiently break public-key cryptosystems such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), jeopardizing data confidentiality and integrity at the edge, fog, and cloud layers. Resource-constrained IoT devices in logistics, such as RFID scanners and GPS trackers, are especially vulnerable because their limited computational power prevents them from adopting robust, quantum-resistant encryption. Fog nodes aggregate and process data locally for real-time decision-making, becoming prime targets for quantum-enabled attacks that could disrupt logistics operations. Moreover, centralized cloud systems storing vast amounts of sensitive logistics data face the risk of having their data decrypted by quantum adversaries, who may also intercept and store encrypted communications now, anticipating future quantum capabilities to exploit them. These quantum threats can disrupt logistics by manipulating shipment data to cause misdeliveries, turning off critical infrastructure to halt operations, and gaining unauthorized access to networks, leading to data breaches or sabotage [13][14].

3.4.12. Malicious Code Injection

Malicious code injection poses a significant threat to EFC computing architectures in smart logistics systems, primarily because of their decentralized structure and extensive use of IoT devices. Cyber adversaries exploit vulnerabilities across all layers—Edge (IoT devices and sensors), Fog (localized processing and storage), and Cloud (centralized data processing)—to inject unauthorized code that alters system behavior, steals data, or disrupts operations. In early 2025, authorities, including Microsoft's Digital Crimes Unit and Europe, dismantled the Lumma infostealer malware infrastructure, which had compromised over 394,000 Windows systems and targeted sensitive data, such as credentials and financial information. Around the same time, fog ransomware emerged as a significant threat, executing double extortion attacks on organizations such as Fligno in the Philippines and compromising 5GB of sensitive data. This ransomware's ability to infiltrate both

Windows and Linux systems underscores its threat to diverse IT environments. Moreover, the surge in poorly secured IoT devices—33% of which are expected to be vulnerable by 2024—has fuelled the growth of botnets such as Mozi and Gafgyt, which conduct DDoS attacks and data exfiltration, further endangering smart logistics operations [12].

3.4.13. Eavesdropping attacks

Eavesdropping attacks pose a significant threat to the confidentiality and integrity of data in EFC computing architectures, particularly within smart logistics systems. These attacks exploit the distributed and resource-constrained nature of such environments, making them vulnerable to unauthorized data interception. As data flow from edge devices (such as sensors and actuators) to fog nodes and eventually to cloud servers for storage and analytics, the reliance on wireless communication and system decentralization increases exposure to eavesdropping. Attackers can intercept IoT sensor data by monitoring goods, vehicles, or storage conditions, gaining access to sensitive information. They may also compromise fog nodes by exploiting weak security measures to access locally processed data. Furthermore, attackers can conduct MitM attacks by inserting themselves between devices to intercept or modify data packets, thereby undermining data integrity and confidentiality. In smart logistics, unauthorized access to RFID tags and inventory sensors can lead to industrial espage, enabling competitors to gain insights into stock levels and supply chain operations [12][18].

3.4.14. Spoofing attacks

Spoofing attacks in smart logistics exploit the distributed architecture of EFC systems by impersonating legitimate devices or services, compromising data integrity, disrupting operations, and eroding trust across the supply chain. Attackers often pose as edge devices, such as RFID readers or IoT sensors, to inject false data, including spoofed RFID signals that misrepresent the location or status of goods, resulting in inventory errors and misrouted shipments. These attacks target weaknesses in device authentication protocols and often evade detection without strong security measures. In fog computing environments, malicious actors may impersonate legitimate fog nodes to gain unauthorized access, intercept communications, alter data streams, or deny services. The decentralized and dynamic nature of fog networks increases their vulnerability when authentication and trust mechanisms are inadequate. Similarly, attackers use global navigation satellite system (GNSS) spoofing to broadcast counterfeit signals that mislead GPS receivers, causing vehicles or assets to miscalculate their positions. In logistics, this tactic can result in misrouted deliveries, theft, or accidents—for example, by redirecting a delivery truck to the wrong location, causing delays or loss of goods [12][28][29].

3.4.15. Physical security breaches

Physical security breaches in EFC computing architectures pose a significant threat to smart logistics systems, compromising data integrity, disrupting operations, and resulting in financial losses. The distributed nature of these systems, particularly the deployment of edge devices such as sensors, gateways, and RFID tags in remote or unsecured environments, increases their vulnerability to tampering, theft, and unauthorized access. Attackers can exploit default credentials, physically access devices to extract or alter data, and inject malicious code. While essential for processing data closer to the source, fog nodes often lack adequate physical protection, making them targets for hardware manipulation and impersonation attacks that disrupt device communication and compromise data. Although cloud data centers offer better physical security, misconfigurations, such as those reported by Toyota in May 2023 and DarkBeam in September 2023, continue to expose sensitive data. These breaches can result in operational disruptions, such as misrouted shipments, inaccurate inventory tracking, and significant financial consequences, including product theft, reputational damage, and legal repercussions [6][15].

3.4.16. IoT device vulnerabilities

Integrating IoT devices into EFC architectures has transformed smart logistics by enabling real-time tracking, predictive maintenance, and supply chain optimization. However, this interconnected environment introduces significant security vulnerabilities across all layers. Many IoT devices ship with default or weak passwords, making them vulnerable to unauthorized access. This was demonstrated in early 2025 when the "Mirai Resurrection" botnet exploited default credentials to compromise over 5 million devices, including industrial sensors and smart TVs, and launch a global DDoS attack. Compounding this issue, many devices lack mechanisms for regular security updates; a high-profile cyberattack in early 2025 exploited unpatched firmware in smart home systems, hijacking thousands of devices for another DDoS attack. Insecure communication protocols expose IoT systems to interception and manipulation, especially when fog nodes aggregate data without secure methods. Although fog computing decentralizes processing, it also increases the risk of data tampering and exposure, emphasizing the need for verifiable computation techniques to protect data integrity. Cloud centralization makes large volumes of aggregated data vulnerable to breaches, underscoring the importance of robust encryption and access controls. Cyber attackers increasingly target supply chain networks, as seen in 2024, when the QakBot trojan enabled ransomware deployment across U.S.-based manufacturing and retail sectors. In mid-2025, attackers exploited insecure APIs and weak backend security in smart city infrastructures across Europe and North America, leading to disruptions in traffic and emergency services. Retail IoT systems, including point-of-sale terminals, also face risks from DDoS attacks, which can

lead to significant financial losses and reputational damage. The short lifespan of IoT devices and limited support for legacy systems worsen these issues. In 2024, researchers found vulnerabilities in approximately 33% of IoT devices—up from 14% in 2023—facilitating the rise of botnets such as Mozi and Gafgyt, which attackers used to disrupt industrial and logistics systems [11].

3.4.17. Firmware and software vulnerabilities

Firmware and software vulnerabilities in EFC computing architectures pose significant security challenges for smart logistics systems, which rely on real-time data processing and interconnected devices. Outdated firmware on edge devices such as sensors and actuators—often left unpatched owing to infrequent updates—exposes systems to known exploits. For example, in 2025, attackers leveraged unpatched smart home devices to launch a DDoS attack, underscoring the dangers of neglecting firmware updates. Complex supply chains in edge computing further increase risk, as attackers can introduce compromised components into systems; the UK's National Cyber Security Centre attributes 40% of cybersecurity breaches to supply chain weaknesses. Edge devices deployed in remote or unsecured areas are vulnerable to physical tampering, which enables attackers to extract data or install malicious firmware. Fog nodes, which handle data closer to the source, often rely on insecure communication protocols, making them vulnerable to MitM attacks. The lack of standardization across diverse devices and protocols in IoT ecosystems creates interoperability issues and security gaps. In fog computing, inadequately secured middleware can also become a target, allowing attackers to hijack sessions or inject malicious code [30]. Fig. 7 illustrates the security threats, attacks, and vulnerabilities that EFC computing faces in smart logistics.

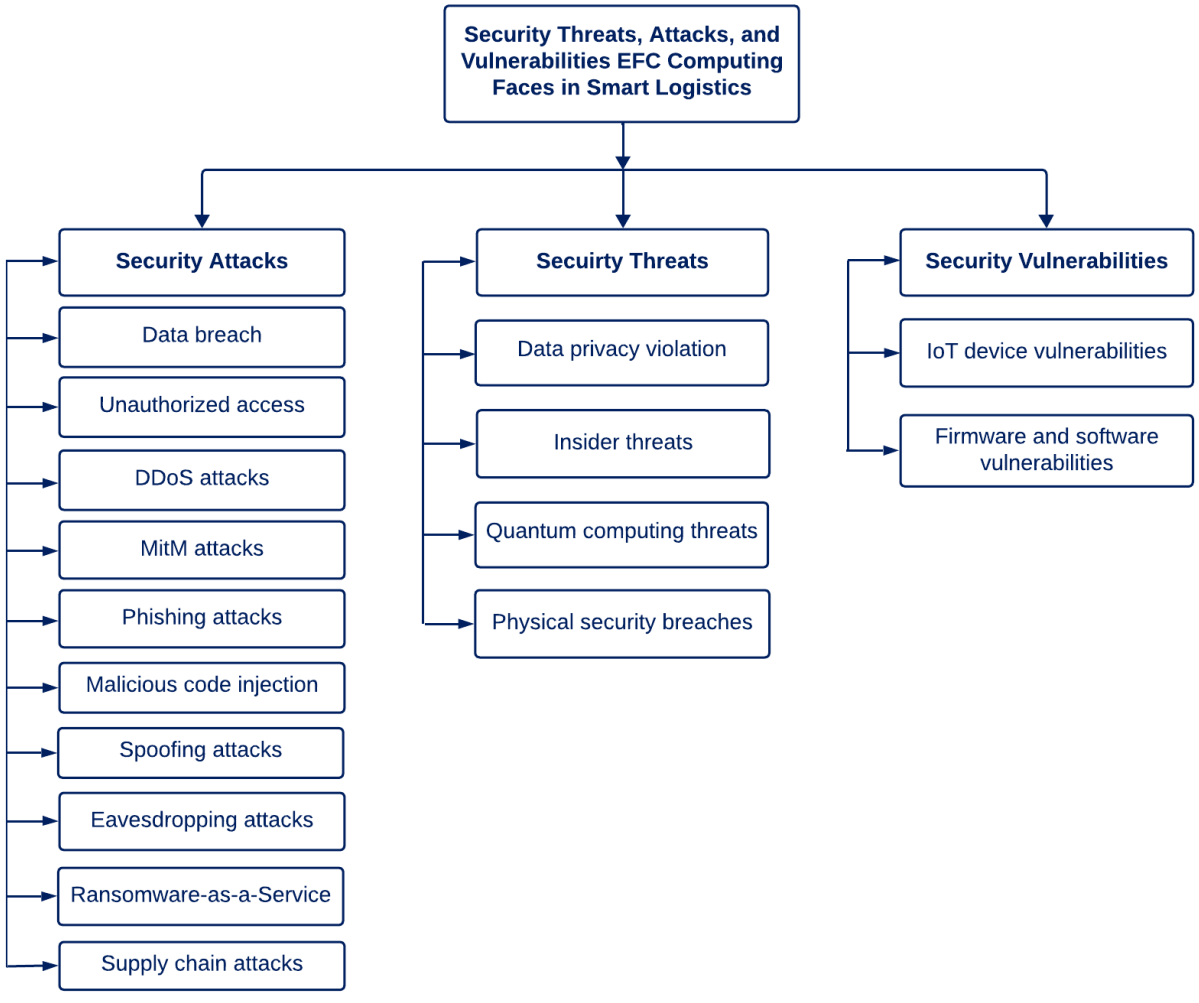

Fig. 7. illustrates the security threats, attacks, and vulnerabilities faced by EFC computing in smart logistics.

3.5. The Concept of Blockchain Technology

Blockchain technology is a distributed ledger system that records and verifies transactions across multiple nodes in a decentralized network [31-33]. Unlike traditional centralized systems, blockchain relies on cryptographic methods to ensure

data transparency, security, and immutability. Each block in the chain contains a set of transactions linked to the previous block, forming a secure and tamper-resistant chain [31-33]. Blockchain has become a transformative technology with applications across finance, supply chains, healthcare, and logistics, enabling trust and automation without the need for central intermediaries. Blockchain technology operates on three core principles that enhance its effectiveness in logistics: decentralization, immutability, and smart contracts. Decentralization distributes data and control across multiple nodes rather than relying on a central authority, thereby increasing security and minimizing the risk of data breaches or system failures [31-33]. In logistics, this decentralized structure fosters transparency and trust among stakeholders, eliminating the need for a central validating entity [34]. Immutability ensures that data on the blockchain cannot be altered or deleted once recorded, owing to cryptographic hashing and consensus mechanisms [31-33]. This feature enables smart logistics systems to maintain a reliable, tamper-proof audit trail of shipments and transactions [34]. Smart contracts, the third principle, are self-executing agreements encoded on the blockchain that trigger actions automatically when predefined conditions are met. These contracts eliminate intermediaries and streamline processes such as payments, compliance checks, and delivery verification [31-34].

The key blockchain platforms in smart logistics include the following.

- Ethereum (ETH): This is a prominent blockchain platform known for its robust support of smart contracts and decentralized applications (dApps). Its upgrade to Ethereum 2.0 in 2022 introduced a proof-of-ake (PoS) mechanism, significantly enhancing scalability and reducing energy consumption. In smart logistics, Ethereum is utilized to automate supply chain agreements, enable secure tokenized transactions, and provide real-time shipment tracking, thereby improving transparency and efficiency.
- Hyperledger Fabric: This is a permissioned blockchain framework for enterprise-level use. Its modular design supports private transactions, making it ideal for secure, controlled environments. Smart logistics is widely adopted in consortium-based systems, where trusted partners require confidential and auditable collaboration across the supply chain [35][36].
- Solana (SOL): Solana is distinguished by its speedy transaction processing and minimal fees, supported by its innovative proof of history (PoH) consensus mechanism. This high-throughput capability is advantageous in smart logistics scenarios that demand rapid data exchange, such as live shipment tracking and inventory updates.
- Polkadot (DOT): Polkadot enables interoperability among diverse blockchain networks through its unique parachain infrastructure. This architecture enables seamless data and asset transfer between chains, which is crucial in smart logistics environments that integrate multiple platforms and require unified communication across supply chain networks.
- Cardano (ADA): Cardano adopts a research-intensive approach to blockchain development, focusing on security, scalability, and sustainability through its Ouroboros consensus algorithm. In smart logistics, Cardano is beneficial for building secure, scalable applications that require data integrity and formal verification, such as tracking systems and compliance management.
- Binance Smart Chain (BSC): The Binance Smart Chain is recognized for its high-speed operations and low transaction fees, providing compatibility with the Ethereum Virtual Machine (EVM). This enables smart logistics developers to easily migrate Ethereum-based applications, benefiting from improved performance and reduced costs, which aids in tasks such as shipment tracking and digital asset management.
- Avalanche (AVAX): Avalanche offers a highly scalable platform with rapid transaction finality, utilizing a novel consensus protocol that supports decentralized finance and enterprise use cases. For smart logistics, this ensures real-time processing and adaptability for systems that require quick decision-making and broad functionality, such as automated warehousing and route optimization.
- Cosmos (ATOM): Cosmos is often referred to as the "Internet of Blockchains" because of its interblockchain communication (IBC) protocol, which promotes interoperability across various blockchain ecosystems. In smart logistics, Cosmos facilitates the exchange of assets and information between various systems, enhancing coordination and enabling end-to-end supply chain visibility.

3.6. Federated Learning

Federated learning is a decentralized machine learning approach in which models are trained across devices or servers that hold local data without sharing it. Unlike traditional centralized methods, FL enhances privacy, reduces latency, and optimizes computational resources by enabling decentralized model training across multiple devices or servers without requiring the sharing of raw data [37-40]. In FL, individual clients train models locally via their data and send only model updates, such as gradients, to a central server, which aggregates these updates to form a global model. This process ensures that data remain private and never leave their source [41-43]. The training begins when the central server distributes an initial model to participating clients. Each client then trains the model on its local data and returns the updates to the server. The

server aggregates these updates into a new global model and redistributes it to clients, repeating the process until convergence is achieved [44-46]. This ensures data privacy and security by keeping raw data on local devices until the model meets performance criteria, such as accuracy [19]. Fig. 8 illustrates the five essential steps in FL [47].

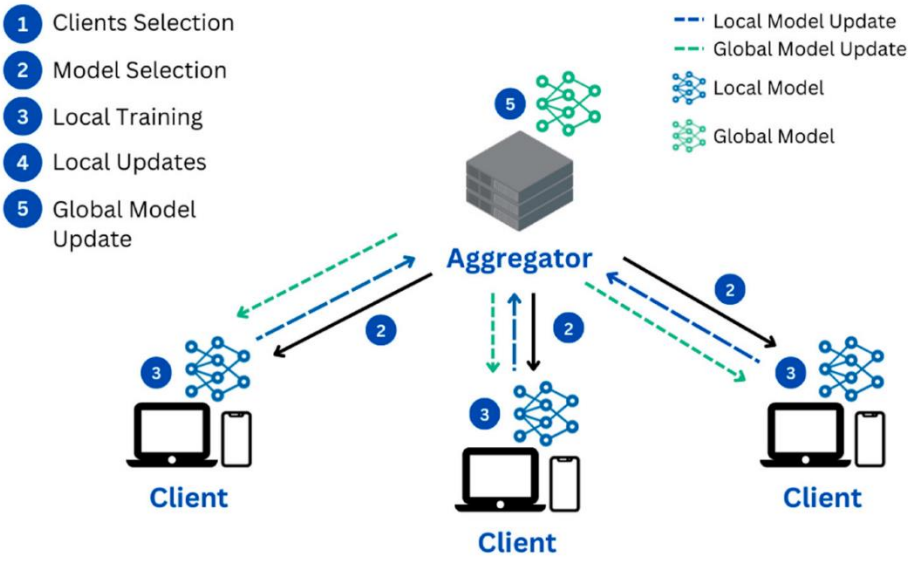

Fig. 8. Illustrates the five essential steps in FL [47].

FL is especially valuable in sensitive and distributed domains, such as logistics, healthcare, and finance [48]. It operates in three primary forms: horizontal FL (HFL), where similar data types are distributed across different entities, such as credit card transactions from various banks; vertical FL (VFL), where different data types exist for the same entities, such as encrypted healthcare records from one hospital; and transfer FL (TFL), which facilitates knowledge transfer across differing data distributions, such as adapting sentiment models across languages [37][49-52]. By decentralizing data management, this approach enhances privacy and mitigates the risks linked to centralized data storage [53][54].

3.6.1. Advantages of FL in Distributed Systems

Federated learning significantly advances machine learning by addressing the challenges of data privacy, security, and efficiency in distributed systems. By adopting a decentralized approach, FL preserves individual data privacy while harnessing the computational capabilities of edge devices. This combination makes FL a powerful and promising solution for many applications in our increasingly interconnected world. Below are the advantages of FL in distributed systems. Table 3 summarizes the advantages of FL in distributed systems.

TABLE III. SUMMARY OF THE ADVANTAGES OF FL IN DISTRIBUTED SYSTEMS.

S/No	Advantages	Description	References
1	Privacy preservation	By keeping data on local devices and only sharing model updates, FL minimizes the risk of exposing sensitive information, which is crucial in domains such as logistics.	[55]
2	Reduced latency and bandwidth usage	FL reduces the data transmitted by sharing only model parameters, resulting in lower latency and decreased bandwidth usage, which is ideal for environments with limited connectivity.	[55]
3	Scalability	FL can scale effectively across multiple devices, enabling the development of models from diverse data sources without the need for centralized data collection.	[55]
4	Enhanced security	FL decentralizes data storage and processing, limiting the potential damage from data breaches. The global model remains secure even if a device is compromised.	[55][56]
5	Reduced data ownership concerns	FL enables data owners to retain complete control over their data without sharing it with third parties, addressing concerns about data ownership and control.	[55][56]
6	Fault tolerance	FL can tolerate device or node failures during the training process, as the model can still be updated using data from other functioning devices, enhancing system resilience.	[55]
7	Improved personalization	By training models locally on devices, FL enables the creation of more personalized models that can better adapt to the unique data patterns of individual users or devices.	[55]
8	Efficient resource utilization	FL leverages the computational power of local devices, thereby reducing the need for central processing and minimizing infrastructure costs associated with servers or cloud services.	[5]
9	Compliance with data regulations	FL helps ensure compliance with data privacy regulations, such as the GDPR, since data does not leave local devices, thereby preventing breaches of regulatory requirements.	[55]

3.7. Convergence of Blockchain Technology, FL, and EFC Computing in Smart Logistics

The convergence of blockchain, FL, and EFC computing in smart logistics is a frontier that aims to optimize supply chain management, improve data privacy, and enhance operational efficiency. Below is an exploration of each concept, the interdependencies, and the complementary strengths.

3.7.1. Overview of edge/fog computing in smart logistics

Edge and fog computing enhance logistics by enabling real-time, localized data processing, reducing reliance on centralized cloud servers, and minimizing latency. By processing data closer to its source, EFC improves fleet management through dynamic route adjustments, enhances warehouse automation with robotics and real-time inventory tracking, and ensures cold chain monitoring by promptly detecting and addressing temperature fluctuations. It also supports predictive maintenance, reduces downtime, and strengthens security and privacy by minimizing cyber risks through decentralized data processing. Additionally, EFC optimizes port and terminal operations by streamlining container management, automating processes, and reducing congestion. EFC significantly increases logistics efficiency and responsiveness by reducing bandwidth and storage costs while enhancing decision-making [57].

3.7.2. Overview of the Blockchain in Smart Logistics

Blockchain is pivotal in smart logistics because it enables a decentralized, immutable ledger that ensures transparent and secure transactions throughout the supply chain. It supports real-time tracking of goods, verifies transactions, and safeguards data integrity—functions that are especially crucial for high-value items or sensitive products, such as pharmaceuticals and perishables. Smart contracts built on a blockchain can automatically trigger actions, such as releasing payments upon delivery, streamlining operations, and minimizing delays and human error. By maintaining an immutable transaction record, blockchain enhances transparency, reduces fraud, and significantly lowers the risk of counterfeiting in global logistics [58].

3.7.3. Overview of Federated Learning in Smart Logistics

As a distributed machine learning approach, FL addresses the need for secure data usage in smart logistics. It enables different entities within the logistics ecosystem (e.g., shippers, warehouses, suppliers) to collaboratively train machine learning models without exposing sensitive data to centralized servers. FL ensures that data remain on local devices (e.g., trucks, sensors, and warehouses), thereby preserving privacy, which is especially useful in logistics, where companies must maintain the confidentiality of both customer and operational data. FL enables supply chain entities to collaborate on building more innovative logistics models to optimize delivery routes, predict demand, or assess risks without sharing proprietary data. For example, a logistics company could train models to predict delays via data from multiple partners without revealing sensitive business information. FL, combined with edge computing, enables the real-time processing of data at the source, thereby reducing latency and enhancing the responsiveness of logistics systems [59][60].

3.7.4. Interdependencies and Complementary Strengths

- **Blockchain and Federated Learning**

Blockchain provides a decentralized infrastructure to ensure the security and transparency of FL models. The transactions involving model updates or aggregated data are recorded on the blockchain, ensuring that only authorized entities can access them. This is crucial for preventing tampering with the training process and ensuring trust between collaborators. FL, in turn, enhances blockchain by allowing participants to improve shared models without revealing their private data, thus addressing one of the significant limitations of traditional machine learning, where data privacy is a concern [5][55].

- **Blockchain and edge/fog computing**

Edge computing processes data at the network's edge, minimizing latency and reducing bandwidth demands. Integrating the blockchain makes this edge processing more secure, as the blockchain validates and records transactions locally. This combination is especially valuable in IoT and vehicle fleet management applications. The EFC optimizes data handling at local nodes, whereas the blockchain ensures transparency and auditability, mitigating the risks linked to centralized data storage [55][56].

- **Federated Learning and Edge/Fog Computing**

FL and edge computing are deeply intertwined in smart logistics, where real-time data must be processed and models continuously updated. EFC provides the infrastructure for FL to run models locally on edge devices, and FL enhances EFC by using federated models for local predictions.

The combination allows for continuous learning and adaptation in real-time logistics applications, such as dynamic route optimization and predictive maintenance [37][57]. Table 4 summarizes the complementary strengths of blockchain, FL, and EFC computing in smart logistics.

TABLE IV. SUMMARY OF THE COMPLEMENTARY STRENGTHS OF BLOCKCHAIN, FL, AND EFC COMPUTING IN SMART LOGISTICS.

S/No	Complementary Strengths	Blockchain	FL	EFC	References
1	Enhanced security and privacy	Ensures data integrity and transparency by recording all transactions and model updates.	Maintains privacy by allowing participants to collaborate on models without sharing private data.	Minimizes data transmission to centralized servers, thus reducing exposure and protecting sensitive logistics data.	[19]
2	Operational efficiency and scalability	Automates processes through smart contracts, reducing administrative overhead and ensuring secure, transparent transactions.	Enables the collaborative optimization of models without exposing sensitive data, thereby fostering scalability across multiple participants.	Ensures efficient, real-time processing of vast datasets by performing computations at local nodes, thereby reducing latency.	[19][60]
3	Automated logistics management	Provides secure, auditable transactions for autonomous logistics systems, such as vehicles and drones.	Supports real-time learning and updates, making autonomous logistics operations more adaptive and efficient.	Processes data in real-time at the edge, enabling the autonomous operation of vehicles, drones, and logistics systems.	[19][60]
4	Integrated approach for logistics optimization	Decentralizes the trust mechanism, allowing for secure and transparent transactions across global logistics.	Enables collaborative and privacy-preserving learning in a distributed manner.	Facilitates local, real-time data processing and decision-making, optimizing logistics systems across global supply chains.	[19][60]
5	Transparency and traceability	Blockchain ensures full traceability of goods throughout the supply chain, increasing transparency in logistics.	FL can enhance model transparency by implementing transparent and auditable processes for training and model updates.	EFC facilitates local processing and real-time monitoring of goods, enhancing visibility across the supply chain.	[19]
6	Real-time decision making	Blockchain's decentralized nature enables real-time verification of transactions and events in the supply chain.	FL enables real-time updates and decision-making by continually learning from decentralized data.	EFC processes data at the edge, supporting real-time logistics optimization and route planning decision-making.	[19][60]
7	Cost efficiency	Blockchain eliminates intermediaries, reducing operational costs.	FL minimizes the need for centralized data storage and computation, lowering infrastructure costs.	EFC minimizes the need for centralized cloud infrastructure, helping to cut bandwidth and storage costs.	[19]
8	Fault tolerance and resilience	Blockchain's decentralized nature ensures system reliability even in the case of node failures.	FL ensures that if one node fails, other nodes can update the model, improving fault tolerance.	EFC provides distributed processing, ensuring local systems can continue operating even if other nodes fail.	[19]

3.8. Integration of Blockchain and FL in EFC Environments for Smart Logistics

3.8.1. Framework for Integration

The proposed framework leverages blockchain and FL in the EFC computing environment to build a seamless, efficient, and secure system for smart logistics. It aims to support real-time decision-making, enable privacy-preserving machine learning, and ensure the scalability of distributed logistics applications. The framework integrates these core technologies to address the growing demands of modern logistics systems while maintaining data integrity, operational efficiency, and adaptability. The framework's core components include the following.

- **Edge-Fog-Cloud Computing**

The EFC is the system's backbone, delivering a decentralized computing infrastructure that processes data closer to its source. It distributes workloads across three layers: edge nodes (local, user-operated devices such as smartphones, tablets, desktops, laptops, and nano data centers), fog nodes (intermediate, high-performance networking devices such as routers and switches), and cloud nodes (centralized storage) [15]. Edge devices, located within one or two hops of IoT sensors, support device-to-device connectivity and communicate reliably with the fog layer. Edge nodes—such as IoT devices on vehicles or warehouse sensors—collect real-time data (e.g., temperature, location, and RFID) and perform initial processing tasks such

as triggering alerts or rerouting vehicles. When an immediate action is needed, such as a response to traffic delays, these nodes activate alarms or adjust routes without relying on the Cloud. By running local models through FL, they process data, make decisions, and act quickly while keeping sensitive information, such as GPS coordinates, local to preserve privacy. The fog layer, which is managed by cloud vendors, runs cloud applications, handles computational tasks offloaded from edge devices, and ensures high-speed, stable connections. Fog nodes collect data from multiple edge nodes and use FL to train local models on these aggregated data, sending only model updates—not raw data—to the Cloud. They also interact with the blockchain to log critical events, such as delivery status or route changes, enhancing transparency and security. Additionally, fog nodes can execute smart contracts to trigger actions on the basis of the analysed data, such as confirming deliveries or updating logistics plans. For example, after processing traffic data from several trucks, a fog node can recommend optimized routes for the entire fleet [6][15].

The cloud data store is a centralized archive accessible to the edge and fog layers, supporting reliability and efficient data access [6][15]. Cloud nodes serve as the system's central authority by receiving model updates from fog nodes, aggregating them, and updating the global model. They securely and immutably maintain the blockchain ledger to record all data transactions, including those from fog nodes. In addition to managing smart contracts and monitoring the status of goods in transit, cloud nodes ensure compliance with contractual agreements among logistics partners. They also handle complex processing tasks and deliver advanced data analytics that require substantial computational resources [6][15]. By processing data near its origin, the EFC reduces the network load, minimizes data transfer, and supports mobility for IoT applications through devices such as laptops and smartphones. It also enhances contextual awareness by integrating sensor data on the basis of location or application context. Its decentralized architecture avoids single points of failure and increases reliability by enabling multiple application snapshots to operate simultaneously. These features make the EFC ideal for distributed, network-constrained applications such as connected vehicles, smart logistics, and automated traffic control [57][61].

- **Blockchain Technology**

Blockchain enhances the integrity and transparency of transactions within the logistics ecosystem, which is crucial for tracking goods and verifying their provenance. Leveraging smart contracts automates key logistics processes such as payment processing, delivery confirmation, and route optimization. It also ensures data integrity by making information generated at edge or fog nodes tamper-proof, thereby creating a reliable record of events, such as delivery logs and sensor readings. Additionally, its distributed ledger enables decentralized access to transaction records and operations, reducing dependence on centralized servers [21][23][58]. Its key features include immutability, which prevents data from being altered; smart contracts, which automatically execute agreements between entities; and decentralization, which removes the need for a central authority and enables peer-to-peer interactions [62][63].

- **Federated Learning**

Federated learning enables transportation companies, suppliers, and other entities to train machine learning models collaboratively without sharing sensitive data. Each edge or fog device trains a local model, which is then securely aggregated via privacy-preserving techniques to form a global model. This ensures that proprietary data remain local while supporting real-time adaptation to dynamic conditions such as traffic or supply chain disruptions. FL offers several key advantages: it enhances data privacy by keeping raw data on local devices, enables collaborative learning by allowing multiple nodes to share model updates that improve the global model, and reduces latency by conducting training locally instead of relying on centralized processing [37].

Integrating blockchain with FL enhances security by creating a decentralized, tamper-proof environment. However, FL in IoT environments faces challenges, including communication overhead and limited computational capacity. FL-based smart decision-making (FedSDM) addresses these issues by leveraging EFC computing to optimize real-time processing, reduce latency, and improve decision-making efficiency [64-66]. Despite its advantages, FLC still has high computational costs and scalability limitations. Traditional consensus protocols, such as proof of work (PoW) and practical Byzantine fault tolerance (PBFT), often consume excessive resources or introduce significant communication overhead, which hampers system efficiency. Moreover, increasing block sizes strain network resources as the number of participating nodes increases. To overcome these issues, researchers are exploring new Blockchain-FL integration frameworks that optimize consensus mechanisms and enhance scalability [22]. Fig. 9 illustrates a framework for integrating blockchain and FL in EFC environments for smart logistics.

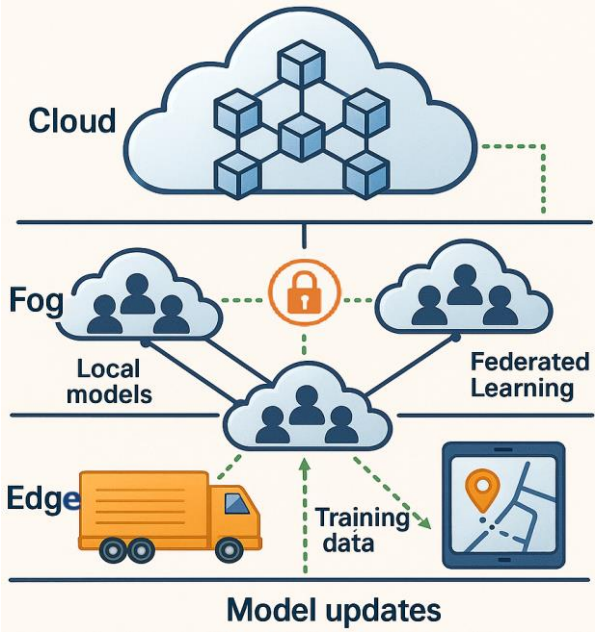

Fig. 9. Illustrates a framework for integrating blockchain and FL in EFC environments for smart logistics.

3.8.2. Data Flow and Interactions between Components

Edge nodes gather real-time data and perform initial processing. If an immediate action is needed, such as in the case of a vehicle delay, edge nodes trigger local responses, such as rerouting vehicles. After processing, they send model updates to the fog nodes, ensuring that the raw data are not transmitted. Fog nodes aggregate data from several edge nodes and process them locally to maintain data privacy. They trained local models and generated model updates, which were sent to the cloud nodes for global aggregation rather than transmitting raw data. Critical events are recorded on the blockchain to ensure transparency and security, and smart contracts can be activated on the basis of the aggregated data. The cloud nodes receive model updates from the fog nodes, aggregate them, and update the global model. They also maintain the blockchain ledger, securely recording all transactions and ensuring compliance. Cloud nodes may handle more complex processing tasks and provide additional analytics to optimize system performance while managing smart contracts to maintain transparency and coordination across the system. Fig. 10 shows the interaction between the blockchain, FL, and EFC components in smart logistics.

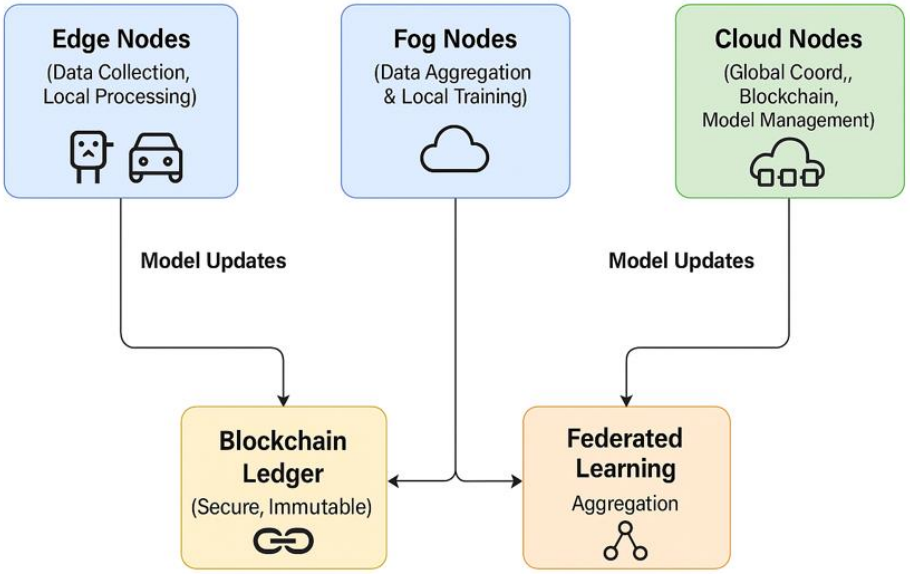

Fig. 10. The interaction between the blockchain, FL, and EFC components in smart logistics.

3.8.3. Technology Stack and Protocols

Smart logistics environments that integrate blockchain and FL within EFC architectures require a sophisticated technology stack to increase data privacy, security, and efficiency in distributed computing systems. This stack includes diverse tools, middleware, application programming interfaces (APIs), and communication protocols that work together to support seamless and secure data exchange.

- **Edge devices**

IoT sensors and mobile devices are primary data sources and initial computational units in smart logistics environments. They collect and locally preprocess data before they participate in FL processes. Edge computing platforms such as EdgeX Foundry and AWS IoT Greengrass support this layer by enabling local data processing, which reduces latency and conserves bandwidth [6][15].

- **Fog nodes**

Fog nodes, situated between edge devices and the cloud infrastructure, offer intermediate computing and storage capabilities that minimize latency and bandwidth usage in smart logistics. They enhance responsiveness and enable localized data processing by bringing computations closer to data sources. Fog computing platforms extend cloud functionalities to the edge, supporting more efficient and timely data handling [6][15][60].

- **Cloud servers**

The cloud infrastructure provides scalable storage and high-performance computing, playing a central role in aggregating trained models and managing the blockchain ledger within smart logistics operations. It handles complex computational tasks that exceed the capabilities of edge and fog nodes, thereby ensuring robust and efficient system performance [19].

- **Blockchain network**

Blockchain technology ensures data integrity and security in the FL ecosystem for smart logistics by providing a decentralized and immutable ledger. Platforms such as Hyperledger Fabric and Ethereum enable key features, including smart contracts and consensus mechanisms. For example, the ChainFL system combines Hyperledger Fabric for subchains with a directed acyclic graph (DAG) based mainchain to increase scalability and performance in FL applications [59][64].

- **Federated learning framework**

FL frameworks enable the decentralized training of models across multiple nodes while preserving data privacy by avoiding the sharing of raw data. Popular tools such as TensorFlow Federated and PySyft, which are open-source libraries designed for secure, privacy-preserving machine learning, support smart logistics workflows. These frameworks empower organizations to collaborate efficiently and compliantly in distributed environments [19][60].

Several tools and technologies facilitate the seamless integration of blockchain and FL in the EFC environments of smart logistics. These include but are not limited to advanced encryption methods, decentralized ledgers, secure multiparty computation, and efficient communication protocols that ensure data privacy and system reliability throughout the logistics process.

- **Consensus algorithms**

In smart logistics applications within EFC environments, integrating blockchain with FL depends on consensus mechanisms such as proof of stake (PoS) and Byzantine fault tolerance (BFT) to validate transactions and model updates. The FLCoin architecture demonstrates this integration through a committee-based Byzantine Fault Tolerant (BFT) consensus protocol, which enhances scalability and operational efficiency [67].

- **Cryptographic techniques**

Researchers employ advanced cryptographic techniques, such as homomorphic encryption and secure multiparty computation (SMPC), to protect data privacy throughout the training and aggregation phases of FL models. These methods maintain the confidentiality of sensitive logistics data, even during distributed and collaborative learning processes [21][68].

- **Smart contracts**

Smart contracts build trust and transparency by automating and enforcing agreements through decentralized mechanisms. In smart logistics FL networks, they govern incentive distribution, impose penalties, and regulate operational rules, thereby enhancing the system's reliability and autonomy [21].

- **Hyperledger Fabric**

Hyperledger Fabric is a modular, open-source blockchain framework managed by the Linux Foundation to support enterprise-grade applications, including smart logistics. It provides high security, privacy, and scalability levels through a permissioned network architecture. Developers can build customized blockchain solutions via their smart contract (chaincode) capabilities. Authorized nodes across the network validate, execute, and record transactions via robust consensus mechanisms, making Hyperledger Fabric well suited for secure and regulated logistics operations [69].

- **TensorFlow Federated (TFF)**

TensorFlow Federated (TFF) is an open-source framework designed to facilitate the development, testing, and deployment of FL algorithms in distributed environments, such as smart logistics. It features two main layers: the FL API, which simplifies model training and evaluation, and the Federated Core (FC) API, which supports the creation of custom algorithms. TFF enables secure and efficient distributed computation and simulation, allowing developers to build and test models across diverse logistics nodes.

- **InterPlanetary File System (IPFS)**

IPFS is a decentralized, peer-to-peer file storage system that enables secure data storage and sharing. Smart logistics FL networks store model parameters and updates, helping maintain data integrity, immutability, and availability across the federated infrastructure [70].

- **Middleware platforms**

These platforms enable seamless interoperability among edge devices, fog nodes, and cloud servers by managing data flow, authentication, and task scheduling. For example, EdgeX Foundry offers a flexible framework for developing and deploying IoT solutions, supporting multiple protocols, and providing microservices for efficient data management. Middleware tools, such as Apache Kafka and RabbitMQ, handle data streams and facilitate communication across distributed components. By addressing the asynchronous nature of FL and supporting the decentralized structure of the blockchain, these platforms play crucial roles in maintaining system efficiency and coherence [71].

- **Application Programming Interfaces (APIs)**

APIs facilitate seamless communication between the FL framework and the blockchain network by enabling the submission of model updates, retrieving global model parameters, and recording transactions on the blockchain. RESTful APIs, which adhere to REST architecture principles, typically serve as the interface connecting FL frameworks, blockchain platforms, and edge devices. These APIs ensure smooth client–server interactions and maintain efficient data flow and control by leveraging standard HTTP methods such as GET, POST, PUT, and DELETE.

- **Communication protocols**

Efficient and secure communication plays a vital role in the integration process, particularly in resource-constrained environments. Protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) enable lightweight data exchange, whereas HTTP/HTTPS supports web-based interactions. For short-range wireless networking, systems often rely on ZigBee and Z-Wave, utilizing Bluetooth low energy (BLE) to connect nearby devices. These protocols collectively enhance the data transfer efficiency in edge environments [72-74].

Integrating blockchain and FL in EFC environments requires a comprehensive technology stack comprising edge devices, fog nodes, cloud servers, blockchain networks, and FL frameworks. Middleware platforms, APIs, and standardized communication protocols facilitate seamless interaction and data flow across these components, strengthening security, privacy, and efficiency in distributed computing applications [23].

3.9. Applications of Blockchain and FL with EFC Computing Environments in Smart Logistics

Smart logistics increasingly relies on advanced technologies to optimize supply chain operations, enhance security, improve efficiency, enable real-time tracking, optimize the supply chain, risk management, autonomous operations, and sustainability. These technologies enhance logistics systems by allowing more efficient, secure, and intelligent decision-making across various domains. Below are brief descriptions of the applications of blockchain and FL within EFC computing environments in smart logistics:

3.9.1. Data security and privacy in smart logistics

Integrating blockchain and FL into EFC environments for smart logistics enhances data security and privacy. Blockchain provides a decentralized, tamper-resistant ledger, whereas FL facilitates collaborative model training without exposing raw data. By combining these technologies, the system effectively addresses key challenges related to data security and privacy [23]. Blockchain and FL provide a robust framework that enhances trust and privacy in AI-driven applications, particularly in smart logistics, where data security is paramount. Blockchain enhances FL by ensuring data integrity, transparency, and security through its decentralized ledger, thereby eliminating reliance on central authorities and reducing single points of

failure [4][75-77]. It maintains immutable training data records and model updates to prevent tampering, whereas consensus mechanisms, such as Proof of Stake, validate transactions to mitigate fraud. Smart contracts automate agreements between FL participants, enforce rules without intermediaries, and enable traceability by creating an audit trail that increases accountability and protects against attacks such as data poisoning and model inversion [78][79].

Moreover, FL preserves privacy by enabling decentralized model training without sharing raw data, employing techniques such as differential privacy, homomorphic encryption, and multiparty computation to secure data exchanges while maintaining accuracy. Despite this, model updates can still risk leaking sensitive information; integrating blockchain addresses this by providing a transparent, immutable framework for secure model sharing. For example, the blockchain-based privacy-preserving and secure FL (BPS-FL) scheme uses threshold homomorphic encryption to ensure that only authorized entities have access to model updates, thereby creating a secure and trustworthy FL ecosystem for smart logistics operations [4][20][46][80-82]. When integrated with FL, blockchain technology creates a robust framework that enhances data security and privacy in smart logistics in the following ways.

- *Data integrity and transparency*: Blockchain technology immutably records data and FL model updates in smart logistics, creating a transparent and auditable ledger. This immutability fosters trust among stakeholders within the EFC computing environment. For example, the Applied Privacy-Preserving FL Blockchain (APPFLChain) architecture combines Hyperledger Fabric with FL to securely facilitate collaborative AI model training while preserving data privacy and integrity [83].
- *Decentralized trust management*: Blockchain's decentralized structure, reinforced by consensus algorithms, removes reliance on a central authority. This design increases fault tolerance and builds trust among distributed entities within smart logistics systems. The blockchain-integrated FL (BIT-FL) framework uses Byzantine fault-tolerant consensus to enable trusted and private collaboration among diverse stakeholders [84].
- *Privacy-preserving model training*: FL trains models locally without exposing raw data, thereby preserving privacy—a critical need in smart logistics. Integrating blockchain further enhances privacy by restricting access to sensitive data and model updates exclusively to authorized parties. The privacy-preserving blockchain-based federated learning (PPBFL) model leverages a blockchain to manage model parameters securely and applies differential privacy techniques to safeguard data throughout the local training process [21].
- *Incentive mechanisms*: Blockchain enables transparent and automated incentive systems that motivate participation in FL processes across logistics networks. For example, the BIT-FL framework integrates these incentive mechanisms to encourage collaboration while ensuring privacy and system security [84].
- *Secure data sharing:* Blockchain strengthens security and traceability in data sharing among entities within smart logistics environments, ensuring that data exchanges occur responsibly and with informed consent. The blockchain-based privacy-enhancing FL approach demonstrates how organizations can leverage blockchain to protect data privacy during collaborative efforts [46].
- *BIT-FL framework*: The BIT-FL framework integrates blockchain technology with Byzantine fault-tolerant consensus and differential privacy to create a secure, privacy-preserving, and incentivized FL environment tailored for distributed logistics operations [84][85].
- *Auditability and transparency*: The blockchain's immutable ledger records every model update and participant interaction in FL systems for smart logistics, enhancing auditability. Maintaining verifiable logs of all modifications ensures model integrity, supports regulatory compliance, and enables thorough traceability—key elements for effective security monitoring [79].
- *Secure model updates*: In smart logistics FL networks, trusted nodes validate updates before integrating them into the global model via blockchain. Consensus protocols prevent fraudulent contributions, ensuring that the model remains reliable and trustworthy [83].
- *Protection against data poisoning*: Blockchain consensus mechanisms enhance resilience against data poisoning attacks by validating every model contribution and monitoring participant behavior to prevent malicious activity. This process safeguards smart logistics FL systems from adversarial data manipulation and ensures model integrity through transparent auditing [23].

3.9.2. Real-time tracking and monitoring

Integrating blockchain and FL within EFC frameworks greatly enhances real-time tracking and monitoring in smart logistics. The blockchain provides a transparent, tamper-proof record of each logistical event, ensuring full traceability for all stakeholders. At the same time, FL enables IoT devices such as sensors and GPS modules to collaboratively train models

without sharing raw data, allowing for accurate predictive maintenance and adaptive route planning. This combined approach optimizes fleet performance and improves on-time delivery [86].

3.9.3. Inventory and supply chain optimization

Blockchain-enabled FL enhances smart logistics by enabling secure, privacy-preserving, and collaborative optimization across the supply chain. FL allows decentralized learning from distributed inventory data while maintaining confidentiality, and blockchain ensures data integrity and traceability. Together, they enhance demand forecasting, facilitate real-time inventory tracking, and improve supply chain responsiveness through robust analytics across multiple data sources [87][88]. Zhu et al. [89] highlighted how secure, decentralized data processing transforms supply chain dynamics, fostering more agile and resilient logistics networks.

3.9.4. Autonomous logistics operations

Integrating blockchain and FL enhances autonomous operations in smart logistics by ensuring secure, private, and efficient system performance. FL enables decentralized model training critical for navigation and coordination, whereas the blockchain secures transaction records and model updates through a tamper-resistant ledger. They support real-time decision-making and collaborative route management among autonomous vehicles [4][5].

3.9.5. Fraud detection and risk management

Blockchain-based FL (BCFL) offers a powerful solution for fraud detection and risk mitigation in smart logistics platforms that manage financial transactions and operational data. By enabling decentralized entities to collaboratively train models without sharing raw data, BCFL enhances fraud detection capabilities while maintaining data privacy. The inherent transparency of the blockchain further strengthens interorganizational trust and security. Research confirms that BCFL significantly enhances fraud prevention in sensitive areas, such as payment systems and credit evaluation, while protecting consumer privacy [90][91].

3.9.6. Sustainability in logistics

BCFL enhances sustainable logistics by enabling secure, efficient, and privacy-aware collaboration among supply chain stakeholders. The FL optimizes routes and resource use in real time without centralizing sensitive data, whereas the blockchain transparently records transactions to support emissions reporting and regulatory compliance. These technologies enhance logistics efficiency, minimize environmental impact, and foster accountability. Researchers also emphasize the blockchain's contribution to increasing supply chain visibility and encouraging responsible practices [49][92-94].

3.9.7. Smart contract automation and data sharing for collaborative learning

Smart logistics ecosystems use blockchain-integrated FL to automate and secure collaborative learning processes. Smart contracts on the blockchain manage tasks such as verifying participants, updating models, processing payments, enhancing transparency, and minimizing manual intervention. By combining IPFS with blockchain, these systems enable secure data exchange while preserving privacy. Incentive mechanisms in smart contracts promote honest participation [80]. Consortium blockchains further increase scalability and synchronization efficiency, strengthening decentralized logistics analytics [77].

3.9.8. Collaborative fleet management and optimization

The convergence of blockchain and FL technologies significantly enhances smart fleet management. Blockchain ensures secure and transparent transaction records for vehicle leasing, toll payments, and insurance processing, whereas smart contracts automate logistics tasks, such as maintenance scheduling and other operational processes. Moreover, FL leverages distributed data from fleet vehicles to power predictive analytics, enabling efficient routing, accurate breakdown prediction, and reduced fuel consumption. These technologies increase fleet reliability and reduce operational downtime [20].

3.9.9. Supply chain transparency and provenance

Blockchain and FL enhance product authenticity and accountability in smart logistics by providing end-to-end traceability and transparent data sharing. Blockchain secures the entire lifecycle of goods—from origin to delivery—on an immutable ledger, which prevents counterfeiting and preserves data integrity [87][88]. Moreover, FL facilitates collaborative data modelling across stakeholders without exposing proprietary information, improving demand forecasting, and minimizing stock discrepancies [75]. Together, these technologies foster trust and enhance transparency throughout the supply chain.

3.9.10. Autonomous delivery systems

Smart logistics integrates blockchain and FL to improve the reliability and efficiency of autonomous delivery systems. Blockchain ensures secure transaction verification and automates processes through smart contracts, whereas FL enables delivery units to learn from distributed traffic and navigation data without compromising privacy [95]. These technologies

optimize route planning, minimize congestion, and increase delivery accuracy. Recent studies have demonstrated that blockchain-FL models enhance vehicular network security and facilitate efficient UAV-based logistics [81][96].

3.9.11. Sustainability and carbon footprint tracking

Integrating blockchain and FL enhances smart logistics operations by improving environmental monitoring and advancing sustainability practices. The blockchain creates verifiable records of carbon footprints and ensures compliance with regulations, whereas FL enables decentralized models to predict emissions and develop reduction strategies. Together, these technologies optimize packaging, reduce energy consumption, and streamline route planning, allowing logistics providers to minimize their ecological impact [82].

The proposed framework makes several key contributions that highlight both its novelty and practical relevance, demonstrating clear advancements in smart logistics and distributed computing systems. These contributions highlight how the research pushes the boundaries of current knowledge while addressing real-world challenges in the field. These contributions include the following.

- *A unified EFC architecture for smart logistics*: This study presents a hierarchical and modular EFC architecture specifically designed for smart logistics scenarios. The architecture distributes the computational load across edge, fog, and cloud layers to support real-time analytics at the edge while allowing for centralized orchestration when necessary. It offers a scalable foundation for managing diverse logistics data sources, enabling responsive and adaptive operations while significantly reducing latency compared with traditional cloud-only models.
- *Integration framework for blockchain and FL in EFC computing environments*: This survey introduces a novel integration model that combines the blockchain's decentralized trust infrastructure with the privacy-preserving features of FL, which are coordinated across EFC layers. This integrated approach fosters secure, trustworthy, and privacy-aware collaborative intelligence within logistics networks, effectively addressing challenges such as data leakage, model poisoning, and accountability gaps.
- *Privacy-preserving model training via FL*: This study uses FL to train predictive and optimization models across various logistics endpoints while maintaining the decentralization of sensitive operational data. This approach safeguards organizational privacy and ensures compliance with regulations such as the GDPR. By enabling multiple stakeholders to collaborate and share insights without compromising confidential data, this method fosters collective intelligence while maintaining data security.
- *Blockchain-based data provenance and trust management*: This study introduces a blockchain layer that secures the entire data pipeline to ensure verifiable data provenance, integrity, and auditability of all transactions, including model updates and IoT sensor data transmissions. By doing so, the system builds trust among noncollaborative parties and minimizes the risk of disputes, fraud, and unauthorized tampering within supply chains.
- *Smart contract automation for logistics operations*: Smart contracts automate key logistics processes, including shipment verification, delivery confirmation, access control, and anomaly detection, by enforcing real-time, rule-based actions that are tamperproof and transparent. They reduce operational overhead, minimize human error, and eliminate process delays by streamlining workflows across organizational boundaries.
- *Lightweight consensus mechanism tailored for edge-fog nodes*: This study develops or adapts a resource-efficient consensus protocol, such as a variant of practical Byzantine fault tolerance or proof-of-authority, optimized explicitly for low-power edge and fog devices. By doing so, it enables the deployment of blockchain in constrained environments and effectively addresses the energy consumption and latency challenges that typically hinder traditional blockchain implementations in logistics.
- *Cross-layer communication protocol for secure model aggregation*: This study designed a secure, low-latency communication protocol that enables federated model updates across edge, fog, and cloud nodes, using blockchain-based verification to ensure the authenticity of each update. This protocol supports efficient and secure multihop coordination of learning tasks and updates, which is essential for managing geographically distributed logistics infrastructures.
- *Roadmap for future research and industrial deployment*: This study highlights key open research directions, including blockchain scalability, FL personalization, regulatory considerations, and integration with legacy logistics infrastructure. Identifying these unresolved challenges and outlining potential technological pathways lays a strong foundation for ongoing interdisciplinary research and drives commercial adoption.

4. CASE STUDIES AND PRACTICAL IMPLEMENTATIONS

Below are some case studies and practical implementations of blockchain and FL in EFC computing environments for smart logistics.

4.1. Maersk and IBM TradeLens Blockchain Project

Maersk and IBM have collaborated to optimize supply chain management in the logistics sector by leveraging blockchain technology through the TradeLens platform. This initiative enhances transparency, traceability, and real-time data exchange among stakeholders. The TradeLens creates a secure, immutable digital record of goods moving through the supply chain, connecting shippers, customs officials, and logistics providers in real time to enable seamless tracking [97].

4.2. Walmart and Blockchain for Supply Chain Traceability

A major retail corporation, Walmart, has adopted blockchain technology to enhance supply chain traceability, particularly in food tracking [98]. By integrating blockchain with IoT sensors and FL, the company strengthens visibility across the entire supply chain—from farm to store. Blockchain offers end-to-end traceability, whereas FL processes decentralized data from farms, warehouses, and distribution centers to enhance demand forecasting and inventory management [99]. Walmart's blockchain integration for food supply chain traceability demonstrated remarkable efficiency, cutting the time required to trace food origins from days to seconds. This system also improved inventory accuracy and reduced food waste by 15% through enhanced demand prediction models powered by FL [98].

4.3. DHL and Blockchain for Smart Logistics

DHL has adopted blockchain-based solutions to enhance supply chain transparency, reduce fraud, and optimize logistics operations. By using blockchain technology, the company securely tracks every movement of goods and provides stakeholders with real-time access to transaction data. It also uses FL to enhance predictive models for route optimization and load balancing, thereby improving the efficiency of transportation and warehousing [100]. Joint research by DHL and Accenture reveals that blockchain transparency can reduce order processing times by up to 65% and decrease data entry requirements by approximately 80%. Similarly, Transport Systems Catapult (2023) reported that blockchain-enabled tracking lowered cargo theft by 38% in pilot programs and accelerated insurance claim processing by over 40% [101-103]. These improvements led to a better customer experience and more reliable delivery times, thereby reinforcing trust in the logistics network. In collaboration with Hewlett-Packard Enterprise (HPE), DHL Express developed a blockchain-based invoicing system as a robust alternative to back-end processes. This system facilitated quote approvals, making quotations visible to all network participants [101-103].

5. CHALLENGES AND LIMITATIONS

Integrating blockchain and FL into EFC computing environments for smart logistics offers significant advantages; however, stakeholders must address several challenges and limitations to ensure successful implementation. Below are brief descriptions of some of the challenges and limitations.

5.1. Scalability issues

Scalability poses a significant challenge in implementing blockchain and FL within smart logistics systems built on EFC computing. Blockchain networks struggle with performance due to consensus mechanisms such as proof-of-work or proof-of-ake, which cause transaction delays and disrupt real-time logistics tracking. Moreover, FL demands substantial computational resources to train models across numerous decentralized devices. As the number of participating nodes increases, the communication overhead increases, and managing model aggregation becomes more complex [19][86].

5.2. Interoperability and standardization

Interoperability and standardization pose significant challenges in integrating blockchain and FL into EFC architectures within smart logistics. Stakeholders often use different communication protocols, data formats, and system structures, making seamless data integration difficult. Incompatibilities between blockchain platforms, such as Ethereum and Hyperledger, hinder data exchange. Moreover, the deployment of FL across diverse logistics infrastructures is hampered by variations in hardware capabilities and data types, which obstruct collaborative learning [52][104].

5.3. Security and privacy risks

Blockchain and FL enhance data integrity and privacy, but their use in smart logistics also introduces new security risks. Although tamper resistant, the blockchain remains vulnerable to 51% attacks and smart contract breaches, which can manipulate critical transactional data and disrupt logistics operations. Similarly, FL keeps raw data decentralized but exposes systems to inference attacks, where malicious actors can extract sensitive information from shared model updates, compromising the confidentiality of logistics processes [86].

5.4. Cost and resource constraints

Adopting a blockchain and FL in smart logistics imposes significant cost and resource demands. Blockchain requires substantial computational power to maintain decentralized ledgers and execute consensus algorithms, which makes it financially burdensome, especially for large-scale logistics networks. FL adds to these costs by requiring robust processing

capabilities and stable bandwidths for distributed model training, which strains logistics companies with limited IT infrastructure [86][105].

5.5. Adoption barriers

Organizational resistance, regulatory constraints, and skill shortages hinder the widespread adoption of blockchain and FL in smart logistics. Companies often delay implementation because of concerns about disrupting operations or affecting their workforce. Managing decentralized data while complying with regulations such as the GDPR and HIPAA presents significant challenges. These difficulties increase when organizations handle sensitive logistics data across international borders [86][106][107].

5.6. Network latency and connectivity

The smart logistics systems rely on stable network connectivity to operate efficiently. Data transfers between edge devices, fog nodes, and cloud services often face disruptions in regions with limited bandwidths or unstable connections. These interruptions can degrade the performance of FL models and slow down blockchain transaction validation, ultimately hindering the timeliness of logistics operations [15][108].

5.7. Energy consumption

Blockchain and FL technologies consume significant energy, creating sustainability challenges in logistics applications. Blockchain's energy-intensive consensus mechanisms—especially Proof-of-Work—demand substantial computational resources. Similarly, FL increases energy consumption, particularly on edge devices commonly used for logistics tracking and inventory management. These elevated power requirements directly conflict with the energy efficiency objectives of modern logistics systems [21][86][109].

5.8. Data quality and heterogeneity

The decentralized nature of smart logistics produces diverse datasets from GPS, RFID, sensors, and warehouse systems, often resulting in inconsistent data quality. These variations, such as differing data formats and incomplete records, undermine the effectiveness of FL models, which rely on high-quality, standardized data for accurate training and reliable predictions [110-112].

5.9. Latency and real-time processing

Smart logistics depends on real-time decision-making for route optimization and fleet management tasks. However, delays in aggregating FL model updates and processing blockchain transactions can hinder these time-critical operations. Latency in synchronizing decentralized models or validating blockchain records reduces the responsiveness of logistics services, potentially disrupting their efficiency and reliability [86][105][113].

5.10. System complexity and management

Integrating blockchain and FL into smart logistics infrastructure adds significant architectural and operational complexity. Coordinating distributed devices across edge, fog, and cloud layers demands sophisticated management, while deploying and maintaining FL models across a dispersed fleet of logistics assets consumes substantial resources. Ensuring the decentralization and integrity of blockchain consensus mechanisms also requires continuous oversight [15][86][114].

5.11. Legal and ethical concerns

Blockchain and FL introduce legal and ethical challenges in global smart logistics ecosystems, particularly regarding data ownership, governance, and consent. The immutability of blockchain records can create legal complications during transaction disputes, while FL's decentralized structure makes it challenging to manage and control sensitive data. Stakeholders must address these concerns to ensure compliance and uphold ethical standards in data-sharing practices across logistics networks [115][116].

5.12. Limited consensus on blockchain protocols

In smart logistics, the absence of standardized blockchain protocols fragments the ecosystem, as logistics operators adopt different platforms and consensus mechanisms, such as proof of work (PoW), proof of stake (PoS), or practical Byzantine fault tolerance (PBFT). This divergence hinders interoperability and reduces overall network efficiency. The lack of a unified protocol framework slows broader adoption [117][118].

5.13. Resource availability in edge devices

Smart logistics relies heavily on edge devices, including sensors, GPS trackers, and smart meters. Nevertheless, their limited processing power, storage capacity, and battery life constrain their ability to handle complex FL tasks or perform blockchain

validations. Continuous operation places additional strain on these devices, often resulting in failures or diminished functionality [105][114].

5.14. Limited understanding and expertise

A shortage of professionals skilled in blockchain, FL, and logistics operations limits the deployment of these technologies in smart logistics. Many logistics firms lack the cross-domain expertise necessary to design and manage integrated systems, which hinders innovation and implementation [119][120].

Although integrating blockchain and FL into smart logistics and EFC environments has significant potential, challenges such as data quality, scalability, latency, legal issues, resource constraints, security risks, and standardization hinder progress. Overcoming these obstacles requires ongoing research, close industry collaboration, and the development of standardized solutions and regulatory frameworks to ensure the successful adoption of these solutions.

6. FUTURE RESEARCH DIRECTIONS

Blockchain and FL are transforming smart logistics by enhancing operational efficiency, scalability, security, and environmental sustainability within EFC architectures. As these technologies advance, emerging trends and key development areas shape their wider adoption across the logistics sector. Below are some brief descriptions of future research directions.

6.1. Advancements in Blockchain and FL

Cutting-edge innovations in blockchain are driving the development of more scalable and efficient smart logistics applications. Techniques such as sharding, Layer 2 solutions such as the Lightning Network and Plasma, and consensus mechanisms including Proof-of-Authority (PoA) and Delegated Proof-of-Stake (DPoS) provide energy-efficient alternatives tailored to logistics systems [19][60]. Moreover, advancements in FL, with improved model aggregation and enhanced edge computing, enable adaptive learning across diverse logistics devices. Together, these technologies facilitate real-time decentralized decision-making, breakdown data silos, and boost logistics performance by reducing latency [121].

6.2. Integration with emerging technologies

The convergence of blockchain and FL with cutting-edge technologies such as 5G, IoT, AI, and augmented reality will significantly advance smart logistics. By leveraging 5G and edge computing, logistics systems achieve ultralow latency and localized data processing, which enhances real-time responsiveness and security [114][122][123]. AI enhances automation and forecasting by analysing decentralized data from FL, whereas augmented reality facilitates the dynamic monitoring and control of supply chains. Moreover, blockchain ensures trusted, immutable records for inventory and tracking [124][125].

6.3. Green and sustainable logistics

Blockchain and FL technologies promote environmental sustainability in smart logistics. Blockchain enhances transparency by tracking the carbon footprint across supply chains, holding industries such as pharmaceuticals, food, and retail accountable [126]. Simultaneously, FL analyses decentralized IoT data to optimize energy use and plan smart routes, thereby reducing fuel consumption, minimizing waste, and improving overall fleet efficiency [21][127].

6.4. Policy and regulation development

As blockchain and FL technologies become more prevalent in smart logistics, legal and regulatory frameworks must evolve to ensure privacy, data integrity, and operational transparency. Regulators must define data ownership within decentralized FL systems and enforce privacy laws, such as the GDPR, in global logistics operations. Establishing legal recognition for smart contracts will also enable enforceable digital agreements across international borders [115][128][129].

6.5. Collaborative research opportunities

Collaborative research is crucial in advancing the effective integration of blockchain and FL in smart logistics. Researchers can enhance logistics efficiency across international operations by driving innovations in scalable blockchain protocols and hybrid consensus mechanisms [130][131]. Moreover, progress in FL for decentralized optimization will support the development of high-performing machine learning models that preserve user privacy while enabling intelligent logistics solutions [68].

6.6. Enhanced security and privacy protection

As smart logistics environments gain wider adoption, ensuring strong privacy and security becomes essential. Zero-knowledge proofs and homomorphic encryption enable secure, privacy-preserving data sharing and transactions. These tools are critical in protecting sensitive information related to payments, shipments, and customer interactions [132].

6.7. Cross-industry adoption and interoperability

Smart logistics will increasingly benefit from the widespread cross-industry adoption of blockchain and FL, enhancing interoperability across the automotive, retail, and healthcare sectors. International standardization efforts, driven by organizations such as ISOs, play a crucial role in integrating disparate systems and building cohesive, reliable global supply chains [133][134].

Integrating blockchain and FL into EFC computing environments promises significant advancements in smart logistics. Continued technological innovation, collaborative research, and the development of regulatory frameworks will be essential for overcoming current limitations and establishing a secure, scalable, and sustainable global logistics ecosystem.

7. CONCLUSION

The rapid advancement of smart logistics is reshaping the production, transportation, and delivery of goods in a highly connected, data-driven environment. Central to this transformation is the EFC computing paradigm, which enables scalable, real-time, and intelligent logistics operations. Despite offering robust computational power and data storage capabilities, EFC architectures face a wide range of security threats, including data privacy violations; breaches; unauthorized access; DDoS and MitM attacks; malware; RaaS; supply chain and insider threats; phishing; quantum computing risks; malicious code injections; eavesdropping; spoofing; physical security breaches; and vulnerabilities in IoT devices, firmware, and software. This survey explores how integrating blockchain and FL within EFC computing architectures can transform smart logistics by enabling a seamless, efficient, and secure system. The proposed framework harnesses blockchain and FL to support real-time decision-making, preserve data privacy in machine learning, and ensure the scalability of distributed logistics applications. By leveraging these technologies, smart logistics can enhance data security and privacy, enable real-time tracking and monitoring, optimize inventory and supply chains, support autonomous operations, detect fraud, manage risks, automate smart contracts, and facilitate data sharing for collaborative learning and decision-making. Additionally, the framework promotes collaborative fleet management, improves supply chain transparency and provenance, supports autonomous delivery systems, and enables tracking of sustainability metrics and carbon footprints.

Blockchain and FL offer substantial potential to enhance EFC computing environments in smart logistics. However, they encounter several technical and practical challenges that hinder their seamless integration and widespread adoption. These include scalability limitations, a lack of interoperability and standardization, security and privacy vulnerabilities, and high costs due to resource constraints. Additional barriers include adoption resistance, network latency and unstable connectivity, excessive energy consumption, inconsistent data quality and heterogeneity, and the need for real-time processing. The complexity of system management, unresolved legal and ethical issues, limited consensus on blockchain protocols, constrained resources in edge devices, and a general lack of expertise further hinder their effective implementation.

Future research should advance blockchain and FL, integrate them with emerging technologies, ensure environmentally sustainable logistics, and support the development of effective policies and regulations. Researchers should also prioritize collaborative efforts, strengthen security and privacy protections, and promote cross-industry adoption and interoperability. Integrating blockchain and FL into EFC environments has the potential to revolutionize smart logistics by creating decentralized, secure, and intelligent systems that effectively address the dynamic requirements of Industry 4.0 and future industrial paradigms.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

This research received no external funding.

Acknowledgement

The authors thank the supporting universities for their contribution to this research. We also appreciate the reviewers for their valuable insights and constructive feedback throughout the study. The authors take full responsibility for the views expressed in this manuscript, which do not necessarily represent the official policies or positions of the affiliated institutions.

References

[1] G. D. Raj, and S. Thandayudhapani, "Evolution of e-commerce logistics: Global trends and implementations," *ComFin Research*, vol. 12, no. 2, pp. 42-45, 2024. https://doi.org/10.34293/commerce.v12i2.7466

[2] L. L. Xiang, *"The future of smart logistics: Robotics and AI transforming supply chains by 2030," JUSDA Global*, 2024. Accessed: April. 21, 2025. [Online]. Available: https://www.jusdaglobal.com/en/article/future-smart-logistics-robotics-ai-transforming-supply-chains-2030/

[3] L. L. Xiang, "Smart logistics and digital supply chains: Predicting the next 10 years," *Jusda Global, 2024*. Accessed: April. 21, 2025. [Online]. Available: https://www.jusdaglobal.com/en/article/smart-logistics-digital-supply-chains-next-10-years/?utm_source=chatgpt.com

[4] J. Yu, H. Yao, K. Ouyang, S. Zhang, and Y. Chen, "BPS- Federated Learning: Blockchain-based privacy-preserving and secure Federated Learning," *Big Data Mining and Analytics, vol. 8*, no. 1, pp. 189-213, 2025. https://doi.org/10.26599/BDMA.2024.9020053

[5] B. Yurdem, M. Kuzlu, M. K. Gullu, F. O. Catak, and M. Tabassum, "Federated Learning: Overview, strategies, applications, tools, and future directions," *Heliyon, vol. 10*, no. 19, pp. 1-24, 2024. https://doi.org/10.1016/j.heliyon.2024.e38137

[6] T. Shwe, and M. Aritsugi, "Optimizing Data Processing: A Comparative Study of Big Data Platforms in Edge, Fog, and Cloud Layers," *Applied Sciences*, vol. *14*, no. 1, pp. 1-23, 2024. https://doi.org/10.3390/app14010452

[7] Y. Ding, M. Jin, S. Li, and D. Feng, "Smart logistics based on the Internet of Things technology: An overview," *International Journal of Logistics Research and Applications, vol. 24*, no. 9, pp. 1-23, 2024. https://doi.org/10.1080/13675567.2020.1757053

[8] M. Brunetti, M. Mes, and E. Lalla-Ruiz, "Smart logistics nodes: concept and classification," *International Journal of Logistics Research and Applications*, vol. 27, no. 11, pp. 1984-2020, 2024.

[9] B. Ravi Chandra, K. Kumar, A. Roy, and I. S. Chandra, "Overview of Internet of Things-Based Smart Logistics Systems," In: Prasad, A., Singh, T.P., Dwivedi Sharma, S. (eds) Communication Technologies and Security Challenges in IoT. Internet of Things (pp 241–259). *Springer*, 2024. https://doi.org/10.1007/978-981-97-0052-3_12

[10] B. Bala, and S. Behal, "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges," *Computer Science Review*, vol. 52, pp. 100631, 2024. https://doi.org/10.1016/j.cosrev.2024.100631

[11] S. K. Sahu, and K. Mazumdar, "Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance," *Frontiers in Artificial Intelligence*, vol. 7, pp. 1–16, 2024. https://doi.org/10.3389/frai.2024.1397480

[12] M. A. Q. Al-Riyashi, A. T. Zahary, and F. Saeed, "A review for Fog-Cloud Security: aspects, attacks, solutions, and trends," *Sana'a University Journal of Applied Sciences and Technology*, vol. 2, no. 5, pp. 482–491, 2024. https://doi.org/10.59628/jast.v2i5.1128

[13] T. M. Fernandez-Carames, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *arXiv*, pp. 1-25, 2024. https://doi.org/10.48550/arXiv.2402.00790

[14] J. Coupel, and T. Farheen, "Security Vulnerabilities in Quantum Cloud Systems: A Survey on Emerging Threats," *arXiv*, pp. 1-9, 2025. https://doi.org/10.48550/arXiv.2504.19064

[15] N. Fernando, S. Shrestha, S. W. Loke, and K. Lee, "On Edge-Fog-Cloud Collaboration and Reaping Its Benefits: A Heterogeneous Multi-Tier Edge Computing Architecture," *Future Internet*, vol. *17*, no. 1, pp. 1-23, 2025. https://doi.org/10.3390/fi17010022 (10

[16] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors*, vol. 25, no. 1, pp. 1-45, 2025. https://doi.org/10.3390/s25010079

[17] A. Ali, M. Husain, and P. Hans, "Real-Time Detection of Insider Threats Using Behavioral Analytics and Deep Evidential Clustering," *arXiv*, pp. 1–7, 2025. https://doi.org/10.48550/arXiv.2505.15383

[18] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things-Edge Computing Integration: Challenges, Threats, and Future Directions," *Sensors*, vol. 25, no. 1, pp. 1-42, 2025. https://doi.org/10.3390/s25010213

[19] S. Ren, E. Kim, and C. Lee, "A scalable blockchain-enabled Federated Learning architecture for edge computing," *PLoS ONE, vol. 19*, no. 8, pp. 1-28, 2024. https://doi.org/10.1371/journal.pone.0308991

[20] W. Ning, Y. Zhu, C. Song, H. Li, L. Zhu, J. Xie, T. Chen, T. Xu, X. Xu, and J. Gao, "Blockchain-based FL: A survey and new perspectives," *Applied Sciences, vol. 14*, no. 20, pp. 1-35, 2024. https://doi.org/10.3390/app14209459

[21] H. Li, L. Ge, and L. Tian, "Survey**:** Federated Learning data security and privacy-preserving in edge-Internet of Things," *Artificial Intelligence Review, vol. 57*, no. 130, pp. 1-38, 2024. https://doi.org/10.1007/s10462-024-10774-7

[22] A. A. Ahmed, and O. O. Alabi, "Secure and scalable Blockchain-based Federated Learning for cryptocurrency fraud detection: A systematic review," *IEEE Access*, vol. 12, pp. 102219–102241, 2024. https://doi.org/10.1109/ACCESS.2024.3429205

[23] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing Federated Learning with blockchain: A systematic literature review," *Artificial Intelligence Review*, vol. 56, no. 5, pp. 3951–3985, 2023. https://doi.org/10.1007/s10462-022-10271-9

[24] Y. Tao, "The application of intelligent logistics systems in supply chain management and its challenges: Case studies of automated warehousing and unmanned delivery," *Frontiers in Business Economics and Management*, vol. 16, no. 2, pp. 100-107, 2024. https://doi.org/10.54097/rrxgp164

[25] Archive Market Research, "Smart logistic 2025-2033 overview: Trends, competitor dynamics, and opportunities," *AMR*, 2025. Accessed: May. 21, 2025. [Online]. Available: https://www.archivemarketresearch.com/reports/smart-logistic-56905

[26] R. Dogea, X. T. Yan, and R. Millar, "Implementation of an Edge-Fog-Cloud computing IoT architecture in aircraft components," *MRS Communications*, vol. 13, no. 4, pp. 416–424, 2023. https://doi.org/10.1557/s43579-023-00364-z

[27] D. Manohar, "An introduction to edge computing in the era of connected devices: Bringing data processing closer to sources," *ChatGPT*, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://chatgpt.com/c/67d80972-90f4-800d-ad96-182e2e78f36d

[28] A. Mchergui, R. Hajlaoui, T. Moulahi, A. Alabdulatif, and P. Lorenz, "Steam computing paradigm: Cross-layer solutions over cloud, fog, and edge computing," *IET Wireless Sensor Systems*, vol. 14, no. 5, pp. 157-180, 2023. https://doi.org/10.1049/wss2.12051

[29] J. Sajid, K. Hayawi, A. W. Malik, Z. Anwar, and Z. Trabelsi, "A FOG Computing Framework for intrusion detection of Energy-Based attacks on UAV-Assisted smart farming," *Applied Sciences*, vol. 13, no. 6, pp. 1-23, 2023. https://doi.org/10.3390/app13063857

[30] S. A. Baker, S. J. Rashid, and O. I. Alsaif, "FOG Computing: A comprehensive review of architectures, applications, and security challenges," *NTU Journal of Engineering and Technology*, vol. 2, no. 2, pp. 21–28, 2023. https://doi.org/10.56286/ntujet.v2i2.614

[31] G. Ali, S. Aziku, S. P. Kabiito, M. Zaward, T. Adebo, R. Wamusi, D. Asiku, M. Sallam, M. M. Mijwil, J. Ayad, A. O. Salau, and K. Dhoska, "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends," *Applied Data Science and Analysis*, vol. 2025, pp. 19–82, 2025. https://doi.org/10.58496/ADSA/2025/004

[32] K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G.Ali, "A secure and efficient BlockChain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid energy valley and levy Flight Distributer Optimization algorithm," *IEEE Access*, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

[33] A. Denis, A. Thomas, W. Robert, A. Samuel, S. P. Kabiito, Z. Morish, M. Sallam, G. Ali, and M. M. Mijwil, "A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities," *SHIFRA*, vol. 2025, pp. 1-45, 2025. https://doi.org/10.70470/SHIFRA/2025/001

[34] M. A. Alqarni, M. S. Alkatheiri, S. H. Chauhdary, and S. Saleem, "Use of Blockchain-Based Smart Contracts in Logistics and Supply Chains," *Electronics*, vol. 12, no. 6, pp. 1-14, 2023. https://doi.org/10.3390/electronics12061340

[35] M. Shakila, A. Rama, S. Christy, A. Kanakala, and C. Y. Lau, "Hyperledger Fabric and beyond: A comprehensive review of blockchain innovations in supply chain," *AIP Conference Proceedings*, vol. 3161, no. 1, pp. 1-6, 2024. https://doi.org/10.1063/5.0229280

[36] C.-L. Chen, W.-B. Zhan, D.-C. Huang, L.-C. Liu, Y.-Y. Deng, and C.-G. Kuo, "Hyperledger Fabric-Based Tea Supply Chain Production Data Traceable Scheme," *Sustainability*, vol. 15, no. 18, pp. 1-25, 2023. https://doi.org/10.3390/su151813738

[37] H. M. Taha, M. A. Mohammed, Y. S. Jghef, S. K. Sulaiman, and T. S. Mustafa, "The integration of blockchain technology in 5G-enabled IoT," *2nd International Conference on Applied Computing & Smart Cities (ICACS24)*, Erbil, Iraq, 20-21 May 2024, pp. 1-14. https://doi.org/10.1051/itmconf/20246401001

[38] H. Wang, H. Gao, T. Ma, C. Li, and T. Jing, "A hierarchical blockchain-enabled distributed federated learning system with model-contribution based rewarding," *Digital Communications and Networks*, vol. 11, no. 1, pp. 35–42, 2025. https://doi.org/10.1016/j.dcan.2024.07.002

[39] S. Rahman, S. Pal, Z. Jadidi, and C. Karmakar, "Robust cyber threat intelligence sharing using federated learning for smart grids," *IEEE Transactions on Computational Social Systems*, vol. 12, no. 2, pp. 635–644, 2025. https://doi.org/10.1109/tcss.2024.3496746

[40] M. A. Khan, "Enhancing Grid Resilience Entangled with Federated Learning for Secure Data Aggregation in Smart Grids," *2025 27th International Conference on Advanced Communications Technology (ICACT)*, Pyeong Chang, Korea, Republic of, 16-19 February 2025, pp. 234–240. https://doi.org/10.23919/icact63878.2025.10936689

[41] A. Arya, "Combining Federated Learning and Blockchain to Enhance Cloud Storage Security," *European Journal of Applied Science, Engineering and Technology*, vol. 3, no. 1, pp. 4-16, 2025. 10.59324/ejaset.2025.3(1).01

[42] J. Yu, H. Yao, K. Ouyang, X. Cao, and L. Zhang, "BPS-FL: Blockchain-Based Privacy-Preserving and Secure Federated Learning," *Big Data Mining and Analytics*, vol. 8, no. 1, pp. 189–213, 2025. https://doi.org/10.26599/bdma.2024.9020053

[43] M. Shalan, M. R. Hasan, Y. Bai, and J. Li, "Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection," *Smart Cities*, vol. 8, no. 1, pp. 1–30, 2025. https://doi.org/10.3390/smartcities8010035

[44] A. A. Elshazly, I. Elgarhy, M. Mahmoud, M. I. Ibrahem, and M. Alsabaan, "A Privacy-Preserving RL-Based secure charging coordinator using efficient FL for smart grid home batteries," *Energies*, vol. 18, no. 4, pp. 1–34, 2025. https://doi.org/10.3390/en18040961

[45] R. Shen, H. Zhang, B. Chai, W. Wang, G. Wang, B. Yan, and J. Yu, "BAFL-SVM: A blockchain-assisted federated learning-driven SVM framework for smart agriculture," *High-Confidence Computing*, vol. 5, pp. 1–10, 2025. https://doi.org/10.1016/j.hcc.2024.100243

[46] Z. N. Limbepe, K. Gai, and J. Yu, "Blockchain-Based Privacy-Enhancing Federated Learning in smart Healthcare: a survey," *Blockchains*, vol. 3, no. 1, pp. 1–38, 2025. https://doi.org/10.3390/blockchains3010001

[47] M. A. Asqah, and T. Moulahi, "Federated Learning and blockchain integration for privacy protection in the Internet of Things: Challenges and solutions," *Future Internet*, vol. 15, no. 6, pp. 1–19, 2023. https://doi.org/10.3390/fi15060203

[48] J. Wen, Z. Zhang, and Y. Lan, "A survey on Federated Learning: Challenges and applications," *International Journal of Machine Learning and Cybernetics*, vol. 14, pp. 513–535, 2023. https://doi.org/10.1007/s13042-022-01647-y

[49] Y. Tang, Y. Zhang, T. Niu, Z. Li, Z. Zhang, H. Chen, and L. Zhang, "A survey on Blockchain-Based Federated Learning: Categorization, Application and analysis," *Computer Modeling in Engineering & Sciences*, vol. 139, no. 3, pp. 2451–2477, 2024. https://doi.org/10.32604/cmes.2024.030084

[50] H. Mei, C. Deng, H. Liu, Y. Zeng, and Y. Zeng, "Application of Federated Learning in Smart Grid Fault Diagnosis: Privacy Protection and Efficiency Improvement," *2024 6th International Conference on Energy, Power and Grid (ICEPG)*, Guangzhou, China, 27-29 September 2024, pp. 743–746. https://doi.org/10.1109/icepg63230.2024.10775979

[51] C. Papadopoulos, K. Kollias, and G. F. Fragulis, "Recent advancements in federated learning: state of the art, fundamentals, principles, IoT applications and future trends," *Future Internet*, vol. 16, no. 11, pp. 1–41, 2024. https://doi.org/10.3390/fi16110415

[52] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," *Journal of Big Data*, vol. 12, no. 1, pp. 1–25, 2025. https://doi.org/10.1186/s40537-025-01099-5

[53] D. Suhag, and V. Jha, "A comprehensive survey on mobile crowdsensing systems," *Journal of Systems Architecture*, vol. 142, pp. 102952, 2023. https://doi.org/10.1016/j.sysarc.2023.102952

[54] M. M. Orabi, O. Emam, and H. Fahmy, "Federated Learning: A literature review on decentralized machine learning paradigm," *FCI-H Informatics Bulletin*, vol. 7, no. 1, pp. 15-27, 2025. https://doi.org/10.21608/fcihib.2024.284321.1114

[55] G. Roy, "Federated Learning: A new paradigm in machine learning," *Medium*, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://karliris62.medium.com/federated-learning-a-new-paradigm-in-machine-learning-e3e06ab151a3

[56] K. Hu, S. Gong, Q. Zhang, C. Seng, M. Xia, and S. Jiang, "An overview of implementing security and privacy in FL," *Artificial Intelligence Review*, vol. 57, pp. 1-66, 2024. https://doi.org/10.1007/s10462-024-10846-8

[57] M. Tay, and A. Senturk, "A research on resource allocation algorithms in the context of edge, fog, and cloud," *Materials Today: Proceedings*, vol. 81, pp. 26–34, 2023. https://doi.org/10.1016/j.matpr.2022.11.232

[58] P. Mölle, "Blockchain in logistics: Security and transparency for the supply chain," *DHL Freight Connections*, 2023. Accessed: Feb. 21, 2025. [Online]. Available: https://dhl-freight-connections.com/en/solutions/blockchain-in-logistics-security-and-transparency-for-the-supply-chain/

[59] M. Koch, S. Kober, S. Straburzynski, B. Gaunitz, and B. Franczyk, "Federated Learning for data trust in logistics," *Position Papers of the 18th Conference on Computer Science and Intelligence Systems, ACSIS*, Warsaw, Poland, 17–20 September 2023, pp. 51–58. https://doi.org/10.15439/2023F5947

[60] F. Islam, A. S. Raihan, and I. Ahmed, "Applications of Federated Learning in manufacturing: Identifying the challenges and exploring the future directions with Industry 4.0 and 5.0 visions," *arXiv*, pp. 1-10, 2023. https://arxiv.org/pdf/2302.13514

[61] J. S. Park, "New Technologies and Applications of Edge/Fog Computing Based on Artificial Intelligence and Machine Learning," *Applied Sciences*, vol. 14, no. 13, pp. 1-6, 2024. https://doi.org/10.3390/app14135583

[62] N. R. Pendli, S. Naveen, M. H. Heartlin, R. Kayalvizhi, C. A. Arul, and H. L. Yadav, "Blockchain for Zero-Trust Security Models: A Decentralized Approach to Enterprise Cybersecurity," *Journal of Information Systems Engineering and Management*, vol. 10, no. 33s, pp. 807–813, 2025. https://www.jisem-journal.com/

[63] N. Singh, V. Mittal, V. Rawat, and P. Kumar, "Blockchain Technology: Reshaping Telemedicine and Telehealth Services for Emergency Management," *2025 International Conference on Pervasive Computational Technologies (ICPCT)*, Greater Noida, India, 08-09 February 2025, pp. 619–624. https://doi.org/10.1109/icpct64145.2025.10940394

[64] S. M. Rajagopal, M. Supriya, and R. Buyya, "Leveraging blockchain and Federated Learning in EFC computing environments for intelligent decision-making with ECG data in IoT," *Journal of Network and Computer Applications*, vol. 233, pp. 1-16, 2025. https://doi.org/10.1016/j.jnca.2024.104037

[65] T. Manoj, K., Makkithaya, and V. Narendra, "A blockchain-assisted trusted Federated Learning for smart agriculture," *SN Computer Science*, vol. 6, no. 3, pp. 1-26, 2025. https://doi.org/10.1007/s42979-025-03672-4

[66] F. Liberti, D. Berardi, and B. Martini, "Federated Learning in Dynamic and Heterogeneous Environments: Advantages, Performances, and Privacy Problems," *Applied Sciences*, vol. 14, no. 18, pp. 1-15, 2024. https://doi.org/10.3390/app14188490

[67] W. Zhong, C. Yang, W. Liang, J. Cai, L. Chen, J. Liao, and N. Xiong, "Byzantine Fault-Tolerant Consensus Algorithms: A Survey," *Electronics*, vol. 12, no. 18, pp. 1-25, 2023. https://doi.org/10.3390/electronics12183801

[68] B. Zhao, Y. Ji, Y. Shi, and X. Jiang, "Design and implementation of a privacy-preserving Federated Learning algorithm for consumer IoT," *Alexandria Engineering Journal*, vol. 106, pp. 206-216, 2024. https://doi.org/10.1016/j.aej.2024.06.071

[69] P. B. Patil, and M. Sangeetha, "A comprehensive performance analysis of a Hyperledger Fabric-powered blockchain network for cross-border fund transfers," *Procedia Computer Science*, vol. 233, pp. 723-732, 2024. https://doi.org/10.1016/j.procs.2024.03.261

[70] N. Sangeeta, and S. Y. Nam, "Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability," *Electronics*, vol. 12, no. 7, pp. 1-23, 2023. https://doi.org/10.3390/electronics12071545

[71] A. Bechini, and J. L. Corcuera Bárcena, "Devising an actor-based middleware support to Federated Learning experiments and systems," *Future Generation Computer Systems*, vol. 166, pp. 1-13, 2025. https://doi.org/10.1016/j.future.2024.107646

[72] D. K. Sah, M. Vahabi, and H. Fotouhi, "Federated Learning at the edge in Industrial Internet of Things: A review," *Sustainable Computing: Informatics and Systems*, vol. 46, pp. 101087, 2025. https://doi.org/10.1016/j.suscom.2025.101087

[73] M. Kumar, A. Kaushik, C. Fischione, and V. Sheng, "Standardization and integration of Blockchain and Federated Learning for decentralized edge intelligence in next-generation IoT security," *IEEE Communications Standards Magazine*, 2025.

[74] J. Wu, F. Dong, H. Leung, Z. Zhu, J. Zhou, and S. Drew, "Topology-aware Federated Learning in edge computing: A comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–41, 2024. https://doi.org/10.1145/3659205

[75] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered Federated Learning: Challenges, solutions, and future directions," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–31, 2023. https://doi.org/10.1145/3570953

[76] X. Zuo, M. Wang, T. Zhu, L. Zhang, S. Yu, and W. Zhou, "Federated Learning with blockchain-enhanced machine unlearning: A trustworthy approach," *arXiv*, pp. 1-13, 2024. https://doi.org/10.48550/arXiv.2405.20776

[77] X. Yin, X. Wu, and X. Zhang, "A Trusted Federated Learning Method Based on Consortium Blockchain," *Information*, vol. 16, no. 1, pp. 1-31, 2025. https://doi.org/10.3390/info16010014

[78] B. Chhetri, S. Gopali, R. Olapojoye, S. Dehbashi, and A. S. Namin, "A survey on blockchain-based Federated Learning and data privacy," *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, Torino, Italy, 26-30 June 2023, pp. 1311-1318. https://doi.org/10.1109/COMPSAC57700.2023.00199

[79] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: A comprehensive survey on blockchain-based FL," *Knowledge and Information Systems*, vol. 66, no. 3, pp. 4377–4403, 2024. https://doi.org/10.1007/s10115-024-02117-3

[80] A. Jaberzadeh, A. K. Shrestha, F. A. Khan, M. A. Shaikh, B. Dave, and Geng, J. "Blockchain-based Federated Learning: Incentivizing data sharing and penalizing dishonest behavior. *5th International Congress. BLOCKCHAIN 2023*," Guimarães, Portugal, 12-14 July 2023, pp 186–195. https://doi.org/10.48550/arXiv.2307.10492

[81] S. Sultana, J. Hossain, M. Billah, H. H. Shajeeb, S. Rahman, K. Ansari, and K. F. Hasan, "Blockchain-enabled Federated Learning approach for vehicular networks," *arXiv*, pp. 1-7, 2023. https://doi.org/10.48550/arXiv.2311.06372

[82] M.-V. Vladucu, H. Wu, J. Medina, K. M. Salehin, Z. Dong, and R. Rojas-Cessa, "Blockchain in environmental sustainability measures: A survey," *arXiv*, pp. 1-40, 2024. https://arxiv.org/html/2412.15261v1

[83] T. K. Vashishth, V. Sharma, B. Kumar, K. K. Sharma, S. Chaudhary, and R. Panwar, "Blockchain for securing Federated Learning systems: Enhancing privacy and trust," In P. R. Chelliah, A. M. Rahmani, R. Colby, G. Nagasubramanian, & S. Ranganath (Eds.), Handbook of blockchain for sustainable development (pp. 39-78). Wiley, 2024. https://doi.org/10.1002/9781394219230.ch15

[84] T. Zhang, C. Ying, F. Xia, H. Jin, Y. Luo, D. Wei, X. Yu, Y. Xu, X. Jiang, W. Zhang, and D. Tao, "BIT- Federated Learning: Blockchain-enabled incentivized and secure Federated Learning framework," *IEEE Transactions on Mobile Computing*, vol. 24, no. 2, pp. 1212 – 1229, 2024. https://doi.org/10.1109/TMC.2024.3477616

[85] F. Ren, and Z. Liang, "A data sharing privacy protection model based on Federated Learning and Blockchain technology," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 6, pp. 1317-1326, 2024. https://doi.org/10.14569/IJACSA.2024.01506133

[86] S. M. Rajagopal, S. Muthuraman, and R. Buyya, "Blockchain-integrated FL in EFC systems for IoT-based healthcare applications: A survey," *arXiv*, pp. 1-32, 2024. https://doi.org/10.48550/arXiv.2406.05517

[87] Z. Ma, X. Chen, T. Sun, X. Wang, Y. C. Wu, and M. Zhou, "Blockchain-Based Zero-Trust Supply Chain Security Integrated with Deep Reinforcement Learning for Inventory Optimization," *Future Internet*, vol. 16, no. 5, pp. 1-13, 2024. https://doi.org/10.3390/fi16050163

[88] R. Vettriselvan, C. Vijai, J. D. Patel, R. S. Kumar, P. Sharma, and N. Kumar, "Blockchain embraces supply chain optimization by enhancing transparency and traceability from production to delivery," *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT)*, Pune, India, 22-23 March 2024, pp. 1-6. https://doi.org/10.1109/TQCEBT59414.2024.10545308

[89] L. Zhu, S. Hu, X. Zhu, C. Meng, and M. Huang, "Enhancing the Security and Privacy in the IoT Supply Chain Using Blockchain and Federated Learning with Trusted Execution Environment," *Mathematics*, vol. 11, no. 17, pp. 1-19, 2023. https://doi.org/10.3390/math11173759

[90] T. Baabdullah, A. Alzahrani, D. B. Rawat, and C. Liu, "Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems," *Future Internet*, vol. 16, no. 6, pp. 1-22, 2024. https://doi.org/10.3390/fi16060196

[91] H. Rabbani, M. F. Shahid, T. J. S. Khanzada, S. Siddiqui, M. M. Jamjoom, R. B. Ashari, Z. Ullah, M. U. Mukati, and M. Nooruddin, "Enhancing security in financial transactions: A novel blockchain-based Federated Learning framework for detecting counterfeit data in fintech," *PeerJ Computer Science*, vol. 10, pp. 1-38, 2024. https://doi.org/10.7717/peerj-cs.2280

[92] N. N. Ahamed, and P. Karthikeyan, "Federated Learning Block: A Sustainable Food Supply Chain Approach Through Federated Learning and Blockchain," *Procedia Computer Science*, vol. 235, pp. 3065-3074, 2024. https://doi.org/10.1016/j.procs.2024.04.290

[93] J. Aslam, K. Lai, Y. B. Kim, and H. Treiblmaier, "The implications of blockchain for logistics operations and sustainability," *Journal of Innovation & Knowledge*, vol. 9, no. 4, pp. 1–16, 2024. https://doi.org/10.1016/j.jik.2024.100611

[94] E. Goh, D. Kim, K. Lee, S. Oh, J. Chae, and D. Kim, "Blockchain-Enabled Federated Learning: a reference architecture design, implementation, and verification," *IEEE Access*, vol. 11, pp. 145747–145762, 2023. https://doi.org/10.1109/access.2023.3345360

[95] V. Engesser, E. Rombaut, L. Vanhaverbeke, and P. Lebeau, "Autonomous Delivery Solutions for Last-Mile Logistics Operations: A literature review and research agenda," *Sustainability*, vol. 15, no. 3, pp. 1–17, 2023. https://doi.org/10.3390/su15032774

[96] F. Betti Sorbelli, "UAV-based delivery systems: A systematic review, current trends, and research challenges," *Journal on Autonomous Transportation Systems*, vol. 1, no. 3, pp. 1-40, 2024. https://doi.org/10.1145/36492

[97] A. J. Al Moalem, "Transforming global trade: A case study of Maersk and IBM's TradeLens platform," *LinkedIn*, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://www.linkedin.com/pulse/transforming-global-trade-case-study-maersk-ibms-al-moalem-cepjf/

[98] M. Sharma, and P. Kumar, "Adoption of blockchain technology: A case study of Walmart," In Blockchain technology and applications for digital marketing (pp. 210–225). *IGI Global*, 2024. https://doi.org/10.4018/978-1-7998-8081-3.ch013

[99] C. Wright, "Leveraging blockchain and artificial intelligence in procurement and supply-chain management: A strategic approach for Walmart," *CoinGeek*, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://coingeek.com/leveraging-blockchain-and-artificial-intelligence-in-procurement-and-supply-chain-management-a-strategic-approach-for-walmart/

[100] DHL. "How blockchain technology streamlines the supply chain in logistics," *DHL,* 2023 Accessed: Feb. 21, 2025. [Online]. Available: https://www.dhl.com/discover/en-in/logistics-advice/logistics-insights/how-blockchain-technology-streamlines-the-supply-chain-in-logistics.

[101] S. Lee, "Blockchain in logistics: Enhancing efficiency in supply chains," *Number Analytics,* 2025. Accessed: March. 21, 2025. [Online]. Available: https://www.numberanalytics.com/blog/blockchain-logistics-efficiency.

[102] V. C. Vella, "How blockchain is revolutionizing logistics for SMEs," *DHL*, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://www.dhl.com/discover/en-global/small-business-advice/business-innovation-trends/blockchain-the-future-of-digital-retail.

[103] DHL. "Leveraging blockchain technology to transform logistics," *DHL*, 2024, Accessed: Feb. 21, 2025. [Online]. Available: https://www.dhl.com/discover/en-hk/logistics-advice/logistics-insights/blockchain-technology-in-logistics.

[104] F. Javed, E. Zeydan, J. Mangues-Bafalluy, K. Dev, and L. Blanco, "Blockchain for Federated Learning in the Internet of Things: Trustworthy adaptation, standards, and the road ahead," *arXiv*, pp. 1-9, 2025. https://arxiv.org/abs/2503.23823

[105] L. Albshaier, S. Almarri, and A. Albuali, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities," *Electronics*, vol. 14, no. 5, pp. 1-60, 2025. https://doi.org/10.3390/electronics14051019

[106] T. Ali, and P. Maheshwari, Exploring Blockchain Adoption Barriers: A Systematic Literature Review, Leeds: Emerald Publishing Limited, 2025, pp. 65-159. https://doi.org/10.1108/978-1-83608-756-420251005

[107] L. Rivera, V. Gauthier-Umaña, and C. Chauhan, "Blockchain: An opportunity to improve supply chains in the wake of digitalization," *International Journal of Information Management Data Insights,* vol. 4, no. 2, pp. 1-10, 2024. https://doi.org/10.1016/j.jjimei.2024.100290 (5)

[108] H. A. Alharbi, B. A. Yosuf, M. Aldossary, and J. Almutairi, "Energy and Latency Optimization in Edge-Fog-Cloud Computing for the Internet of Medical Things," *Computer Systems Science & Engineering,* vol. 47, no. 1, pp. 1299-1319, 2023. https://doi.org/10.32604/csse.2023.039367

[109] R. Alami, A. Biswas, V. Shinde, A. Almogren, A. Ur Rehman, and T. Shaikh, "Blockchain enabled FL for detection of malicious Internet of Things nodes," *IEEE Access*, vol. 12, pp. 188174-188185, 2024. https://doi.org/10.1109/ACCESS.2024.3511272

[110] T. Legler, V. Hegiste, A. Anwar, and M. Ruskowski, "Addressing Heterogeneity in Federated Learning: Challenges and solutions for a shared production environment," *Procedia Computer Science*, vol. 253, pp. 2831–2840, 2025. https://doi.org/10.1016/j.procs.2025.02.007

[111] S. Song, Y. Li, J. Wan, X. Fu, and J. Jiang, "Data Quality-Aware Client Selection in Heterogeneous Federated Learning," *Mathematics*, vol. 12, no. 20, pp. 1-17, 2024. https://doi.org/10.3390/math12203229

[112] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous Federated Learning: State-of-the-art and research challenges," *ACM Computing Surveys,* vol. 56, no. 3, pp. 1-44, 2023. https://doi.org/10.1145/3625558

[113] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated Learning: Navigating the Landscape of Collaborative Intelligence," *Electronics*, vol. 13, no. 23, pp. 1-39, 2024. https://doi.org/10.3390/electronics13234744

[114] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *Journal of Network and Computer Applications,* vol. 226, pp. 1-24, 2024. https://doi.org/10.1016/j.jnca.2024.103884

[115] A. K. Tyagi, "Blockchain technology: Values, challenges, and possible applications from an industry perspective," In Human-centric integration of next-generation data science and blockchain technology (pp. 349-367). *ScienceDirect,* 2025. https://doi.org/10.1016/B978-0-443-33498-6.00027-3

[116] G. Rubeis, "Ethical implications of blockchain technology in biomedical research," *Ethik in der Medizin,* vol. 36, pp. 493–506, 2024. https://doi.org/10.1007/s00481-024-00805-w

[117] M. Tangsakul, and P. Sureeyatanapas, "Understanding critical barriers to the adoption of blockchain technology in the logistics context: An interpretive structural modelling approach," *Journal of Open Innovation: Technology, Market, and Complexity,* vol. 10, no. 3, pp. 1-14, 2024. https://doi.org/10.1016/j.joitmc.2024.100355.

[118] A. Kumar Singh, V. R. Prasath Kumar, G. Dehdasht, S. R. Mohandes, P. Manu, and F. Pour Rahimian, "Investigating the barriers to the adoption of blockchain technology in sustainable construction projects," *Journal of Cleaner Production,* vol. 403, pp. 1-18, 2023. https://doi.org/10.1016/j.jclepro.2023.136840.

[119] M. Alimohammadlou, and S. Alinejad, "Challenges of blockchain implementation in SMEs' supply chains: An integrated IT2F-BWM and IT2F-DEMATEL method," *Electronic Commerce Research,* vol. 25, pp. 907–949, 2025. https://doi.org/10.1007/s10660-023-09696-3

[120] Z. Cai, J. Chen, Y. Fan, Z. Zheng, and K. Li, "Blockchain-empowered Federated Learning: Benefits, challenges, and solutions," *arXiv,* pp. 1-28, 2024. https://arxiv.org/html/2403.00873v1.

[121] K. Duan, G. Pang, and Y. Lin, "Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management," *Journal of Digital Economy,* vol. 2, pp. 244-288, 2023. https://doi.org/10.1016/j.jdec.2024.01.005

[122] N. Rane, Ö. Kaya, and J. Rane, "Integrating Internet of Things, blockchain, and artificial intelligence techniques for intelligent industry solutions," In Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry 5.0 (pp. 115–136). *Deep Science* Publishing, 2024. https://doi.org/10.70593/978-81-981271-8-1_6

[123] Z. Taha, C. T. Yaw, S. Koh, S. K. Tiong, K. Kadirgama, F. Benedict, J.-D. Tan, and Y. Balasubramaniam, "A survey of Federated Learning from a data perspective in the healthcare domain: Challenges, methods, and future directions," *IEEE Access,* vol. 11, pp. 45711–45735, 2023. https://doi.org/10.1109/ACCESS.2023.3267964

[124] F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfawaer, M. Alshammari, L. Amouri, S. S. Aljameel, and S. Albassam, "Unlocking a promising future: integrating blockchain technology and FL-IoT in the journey to 6G," *IEEE Access*, vol. 12, pp. 115411–115447, 2024. https://doi.org/10.1109/access.2024.3435968

[125] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, pp. 1-19, 2024. https://doi.org/10.1002/ett.4329

[126] T. H. Hoang, T. T. Tran, and L. N. T. Huynh, "Advances and barriers in promoting green logistics 4.0 from a multi-stakeholder perspective: A systematic review," *Environmental Systems and Decisions,* vol. 45, no. 14, 2025. https://doi.org/10.1007/s10669-025-10006-5

[127] S. Sahoo, S. Kumar, and U. Sivarajah, "Blockchain for sustainable supply chain management: Trends and ways forward," *Electronic Commerce Research,* vol. 24, pp. 1563–1618, 2024. https://doi.org/10.1007/s10660-022-09569-1

[128] S. H. Alsamhi, R. Myrzashova, A. Hawbani, S. Kumar, S. Srivastava, L. Zhao, X. Wei, M. Guizan, and E. Curry, "Federated Learning meets blockchain in decentralized data Sharing: Healthcare use case," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19602–19615, 2024. https://doi.org/10.1109/jiot.2024.3367249

[129] S. Singh, S. B. Verma, B. K. Gupta, and A. Agrawal, "Decentralization and federated approach for personal data protection and privacy control," *Journal of Information and Applied Science,* vol. 19, no. 5, pp. 197-213, 2024. https://doi.org/10.2478/ias-2024-0014

[130] A. Zia, and M. Haleem, "Bridging research gaps in Industry 5.0: Synergizing federated learning, collaborative robotics, and autonomous systems for enhanced operational efficiency and sustainability," *IEEE Access*, vol. 13, pp. 40456–40479, 2025. https://doi.org/10.1109/access.2025.3541822

[131] A. Nazir, J. He, N. Zhu, M. S. Anwar, and M. S. Pathan, "Enhancing IoT security: a collaborative framework integrating Federated Learning, dense neural networks, and blockchain," *Cluster Computing,* vol. 27, no. 6, pp. 8367-8392, 2024. https://doi.org/10.1007/s10586-024-04436-0

[132] P. Whig, R. Sharma, N. Yathiraju, A. Jain, and S. Sharma, "Blockchain-Enabled Secure Federated Learning Systems for Advancing Privacy and Trust in Decentralized AI," *Wiley-IEEE Press*, pp. 321–340, 2024. https://doi.org/10.1002/9781394219230.ch16

[133] S. Bayraktar, S. Gören, and T. Serif, "Blockchain interoperability for future telecoms," *Telecom*, vol. 6, no. 1, pp. 1–29, 2025. https://doi.org/10.3390/telecom6010020

[134] F. Xia, L. Kaiye, W. Songze, and X. Yan, "Enhancing the blockchain interoperability through federated learning with directed acyclic graph," *IET Blockchain*, vol. 3, no. 4, pp. 238–248, 2023. https://doi.org/10.1049/blc2.12033