Journal of Agriculture and Food Research 27 (2026) 102739

Contents lists available at ScienceDirect

Journal of Agriculture and Food Research

journal homepage: www.sciencedirect.com/journal/journal-of-agriculture-and-food-research

TrustFish: A decentralized AI framework for trustworthy end-to-end seafood quality and safety monitoring

Saeed Hamood Alsamhi [a,b,h,*], Raushan Myrzashova [c], Ammar Hawbani [d], Mohammed A.A. Al-qaness [g], Xi Wei [e], Niall O'Brolchain [a], Liang Zhao [d], Mohsen Guizani [f], Edward Curry [a]

[a] Insight Centre for Data Analytics, University of Galway, Ireland
[b] Department of Computer Science and Engineering, College of Informatics, Korea University, Seoul 02841, Republic of Korea
[c] School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui, China
[d] School of Computer Science, Shenyang Aerospace University, Shenyang, 110136, China
[e] Department of Chemistry, University of Science and Technology of China, Hefei, Anhui, China
[f] Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, United Arab Emirates
[g] College of Physics and Electronic Information Engineering, Zhejiang Normal University, Jinhua, 321004, China
[h] Faculty of Engineering, IBB University, Ibb, Yemen

ARTICLE INFO

Index Terms:
Federated learning
Blockchain
Decentralized AI
Seafood
Safety
Quality
Trustworthy
Industry 5.0
Monitoring

ABSTRACT

This paper introduces a novel framework called "TrustFish" to monitor seafood quality and safety, ensuring effective and efficient traceability in the seafood supply chain from fishers to customers. The challenges of seafood traceability include (i) high verification cost, (ii) decentralized structure of the supply chain, (iii) volume of heterogeneous data, and (iv) the lack of fail-safe detection techniques. The TrustFish framework combines decentralized technologies, i.e., federated learning and blockchain, to develop a decentralized, secure, and privacy-preserving system for seafood monitoring in the supply chain. Additionally, data from the supply chain is gathered by Internet of Things devices for monitoring the safety and quality of seafood. In TrustFish, dynamic sharding and directed acyclic graph are used to improve fault tolerance and scalability in diverse supply chain network environments. TrustFish demonstrates how FL and blockchain combine to produce a cooperative, effective, and reliable seafood monitoring. By giving stakeholders access to thorough product histories and environmental circumstances, TrustFish increases consumer trust, decreases contamination, and lowers fraud by allowing stakeholders to access seafood histories and environmental circumstances. The proposed TrustFish solution improves operational effectiveness and public health results while laying the groundwork for the seafood supply chain's advancement in Industry 5.0.

1. Introduction

The seafood supply chain is a vast, diverse, and complex system that faces challenges due to the involvement of various stakeholders, the nature of the product, and its stringent requirements for authenticity and quality. Fragmentation in the supply chain, lack of centralized management, and high monitoring and verification cost all contribute to these challenges. Developing an efficient traceability system for the seafood ecosystem has been very challenging, particularly during the pandemic. To overcome such challenges, stakeholders collaborate and utilize cutting-edge technology. For instance, Ireland is one of the world's biggest seafood producers and exporters, while the salmon from Ireland is regarded as some of the best in the world [1]. Therefore, improving the quality and safety of seafood in the Irish industry will gain a high reputation with the Irish people and ensure worldwide trust. People want to see the provenance of the seafood they buy [2], to ensure seafood safety and fish supplies, seafood consumers and importing nations have recently increased vigilance. Although seafood safety cannot

* Corresponding author. Insight Centre for Data Analytics, University of Galway, Ireland.
E-mail addresses: Saeed.alsamhi@insight-centre.org (S.H. Alsamhi), rose5004@mail.ustc.edu.cn (R. Myrzashova), anmande@ustc.edu.cn (A. Hawbani), alqaness@zjnu.edu.cn (M.A.A. Al-qaness), wxi@ustc.edu.cn (X. Wei), niall.obrolchain@insight-centre.org (N. O'Brolchain), lzhao@sau.edu.cn (L. Zhao), mguizani@ieee.org (M. Guizani), edward.curry@insight-centre.org (E. Curry).

https://doi.org/10.1016/j.jafr.2026.102739
Received 8 August 2025; Received in revised form 30 January 2026; Accepted 1 February 2026
Available online 18 February 2026

be guaranteed due to the presence of chemical materials, seafood dealers and purchasers are cautious about imported seafood goods. Thus, monitoring seafood quality with traceability of security information is essential in fresh seafood systems.

Traceability plays a crucial role in enhancing safety and quality, reducing the cost and risk associated with seafood, and improving the reputation of the seafood industry. Security tracking and and quality of seafood are necessary due to customer demands for a healthy lifestyle [3]. Currently, seafood safety and quality are significant concerns for the seafood industry. Therefore, traceability requirements from manufacturing to distribution are imposed through the supervision and monitoring of seafood safety and quality. The complexity of seafood production and the pollution can occur at any stage. The traceability of seafood is being increasingly highlighted as a solution to the problem of products entering the supply chain that were produced illegally or unethically. Experts increasingly believe that complete supply chain traceability and transparency are the only ways to achieve a safe seafood supply chain, using optimal and intelligent techniques.

Machine Learning (ML) has been proposed to realize early food safety and quality monitoring [4]. However, ML methods suffer from data tampering and centralized processing issues [5], which are barriers to efficient and reliable quality monitoring. The support of edge computing, Internet of Things (IoT), and Federated Learning (FL) can help mitigate some of these challenges. However, federated learning is based on the centralized model coordinator. Training devices are unreliable and have the potential to operate maliciously, which could impact the overall model and result in inaccurate model updates [6]. Therefore, federated learning suffers from reliability, anonymity, and tractability issues (i.e., the use of massive trained models). Furthermore, smart devices may upload inadequate parameters that negatively impact federated learning task performance due to the high communication between smart devices and servers. Therefore, creating a new federated learning architecture reduces transmission loads and enhances the trustworthiness and reliability of model updates. To preserve the local model for efficient verification and to enable traceability verification even when the server collaborates with malicious parties, Homomorphic Encryption (HE) is utilized [7]. However, the scalability of the traceability system remains a challenge in the context of more significant implementation and deployment [8]. Many challenges still exist to impede the widespread adoption of large-scale seafood supply chain systems as listed in Table I.

To overcome these challenges, Table I, various research attempts have explored utilizing Blockchain to facilitate seafood monitoring. However, in addition to improving traceability, smart seafood monitoring systems can also provide more efficiency benefits through a combination of federated learning and blockchain techniques. Blockchain has recently gained tremendous popularity due to its traceability, resistance to tampering, and high-level decentralized security features [14, 15]]. Therefore, the combination of federated learning and blockchain can improve efficiency by eliminating duplication of reconciliation efforts, reducing the need for intermediaries, enhancing end-to-end traceability, and synchronizing transactions.

Table 1
Seafood supply chain challenges.

Challenges	Description
Heterogeneous data	The seafood supply chain comprises massive heterogeneous IoT devices and vehicles with diverse capabilities. Each stage of the seafood supply chain involves heterogeneous devices that collect various data of interest to the consumer, from fisheries and processing to facilities [9, 10]].
lack of transparency	A transparent supply chain presents an image of a seafood industry that is upfront and honest about the processes and trustworthy [11].
Accessibility	It is limited access to data for all involved parties, including stakeholders and consumers [12].
Scalability	The seafood supply chain system requires accommodating many autonomous vehicles and maintaining robustness at a required level, especially in the presence of hacked vehicles, noisy communication channels, and network partitioning [13].

1.1. Motivation and contributions

All stakeholders involved in the seafood supply chain share accurate information and conduct ongoing monitoring to ensure seafood safety and quality from production points to final customers. However, fragmented data, limited transparency, and high verification costs result from the engagement of various stakeholders, heterogeneous IoT devices, and the lack of a uniform data management system. TrustFish addresses the issues and leads to delivering end-to-end traceability, data integrity, and privacy preservation. Unlike existing solutions that treat these technologies independently, the proposed TrustFish framework demonstrates how blockchain and federated learning complement each other: blockchain ensures immutable recording of model updates and monitoring results, while federated learning enables collaborative training without sharing raw data. Privacy is enhanced through the combination of Differential Privacy (DP) and Homomorphic Encryption (HE). DP introduces controlled noise to local model updates, ensuring individual data records cannot be inferred, while HE allows encrypted model aggregation, preventing the coordinator from accessing raw gradients. We also discuss the practical setting of the privacy budget (ϵ) and its trade-off with model accuracy. The key contributions of this paper are as follows:

1) We present TrustFish, a blockchain and FL-based framework for the monitoring of seafood quality and safety, introducing a dynamic consensus algorithm of sharding and a directed acyclic graph (DAG) structure to improve scalability and fault tolerance in heterogeneous IoT environments.
2) We design and implement a privacy-preserving data sharing mechanism using local differential privacy and homomorphic encryption, supported by Hyperledger-based smart contracts to automate compliance verification and guarantee data integrity.
3) We validate TrustFish with a proof-of-concept implementation using synthetic IoT-generated data, demonstrating how real-time monitoring and traceability can help stakeholders detect anomalies and prevent spoilage and fraud.
4) The paper aims to secure a scalable traceability systems in the seafood supply chain, contributing to sustainability and consumer trust.

1.2. Related work

Seafood supply chain systems face challenges (due to the lengthy and fragmented nature of the seafood supply chain) in ensuring trust, transparency, and privacy due to the increasing demand for seafood that prioritizes safety, quality, and sustainability. Seafood is a significant protein source in the human diet and involves heterogeneous IoT devices and multiple stakeholders. In the European Atlantic area, eco-innovation initiatives have been introduced to promote sustainability in the food industry [16]. Such developments have demonstrated that precise traceability systems are crucial for identifying and mitigating safety and quality risks at every stage of the supply chain [17–19].

Blockchain for supply chain traceability: The inherent features of blockchain (i.e., immutability, transparency, and decentralization) made it a prominent solution for supply chain traceability. Several studies have explored how blockchain can track the provenance of goods, including seafood. The authors of [19] discussed blockchain for food traceability, while [20–22] proposed a blockchain for fisheries. Furthermore, in Ref. [23], the authors implemented a blockchain-based traceability system for the fishery supply chain, demonstrating improvements in data integrity and auditability. However, the studies focused on recording transactional data (e.g., location, ownership) and often neglected the continuous, privacy-sensitive environmental data

from IoT sensors that is critical for quality monitoring.

IoT and Federated Learning for Quality Monitoring. IoT sensors deployed to monitor environmental conditions [18,24]. ML models for monitoring and prediction of food safety based on data provided [4]. However, centralized ML approaches require aggregating all sensor data, which leads to privacy, bandwidth, and security issues [5]. Therefore, federated learning enables collaborative model training without sharing raw data. The authors of [6] highlighted FL's for IoT but do not address the specific trust and reliability issues in a multi-stakeholder, adversarial supply chain environment. To improve traceability and dependability from production to consumption, emerging technologies including blockchain, IoT, RFID, and ML have been implemented [25,20]. Federated learning models are nevertheless susceptible to rogue upgrades and faulty devices, notwithstanding the advantages [26].

Integration of Blockchain and Federated Learning: Blockchain and federated learning working together have proven to improve dependability and trust. Blockchain was utilized by frameworks such as *TruFLaaS* [27] and *DeepChain* [28] to generate auditable records of federated learning transactions and encourage involvement. The authors of investigated integration between fog computing and vehicle networks [29]. The research showed that by offering a decentralized verification system, blockchain can lessen FL's susceptibility to malicious upgrades. Nevertheless, blockchain-federated learning systems are not made to meet the demands of a global seafood supply chain in terms of scalability, heterogeneity, and data protection. Blockchain-federated learning frameworks rely on conventional blockchain structures that may suffer from low throughput and high latency when applied to a network of resource-constrained IoT devices. Sharded blockchains have been investigated in other research to increase scalability; for example [29,30–33], showed how to use multi-chain architectures and shard training to overcome the throughput constraints of blockchains in federated learning contexts. However, there is yet no practical use of blockchain-enabled federated learning in seafood supply chains [34,35]. Furthermore, recent studies [36,37] have demonstrated that blockchain-federated learning systems for supply chains are still in the infancy and require further investigation to address issues with scalability, privacy budgets, and real-world heterogeneity.

Three gaps are identified through a review of the literature, which our work aims to address. First, there is a clear need for integrated quality and traceability monitoring; current seafood blockchain systems primarily address custody traceability but lack strong, privacy-preserving mechanisms for incorporating real-time quality inference from IoT sensor data. Second, while blockchain-federated learning systems typically lack a layered privacy strategy, they often provide inadequate privacy protection. The combination of differential privacy and homomorphic encryption for improved secrecy in a supply chain setting remains underexplored. Third, previous studies have not addressed the performance and scalability challenges of deploying a blockchain-federated learning system across heterogeneous and resource-constrained nodes, such as those found in the seafood supply chain. Therefore, TrustFish introduces a novel dynamic sharding consensus mechanism combined with a directed acyclic graph structure to optimize scalability and fault tolerance. A comparative summary of TrustFish framework against key related works is provided in Table II.

2. TRUSTFISH framework

The TrustFish framework combines federated learning and blockchain technologies to create a decentralized, secure, and efficient system to monitor seafood quality and safety throughout the supply chain. Fig. 1 illustrates the architecture of the seafood supply chain, highlighting the integration of IoT devices, FL, and blockchain for end-to-end traceability and accountability. Architecture of the TrustFish framework, illustrating the roles of key stakeholders in the seafood supply chain. Each stakeholder (fisher, transporter, storage, shipper, and retailer) collects IoT sensor data and trains a local federated learning model. To ensure collaborative learning without sharing raw data, model updates are sent to a central aggregator for a global model refinement. End-to-end traceability is provided at the same time as all quality evaluations and transactional data are permanently stored on a Hyperledger Blockchain. In order to ensure openness and confidence, smart contracts automate compliance and allow customers to see the product's whole history.

Environmental factors include temperature and humidity monitoring using smart IoT devices placed in the seafood supply chain, i.e., fishing vessels, transporters, storage facilities, and merchants. To create node-specific models that are aggregated centrally, federated learning processes data locally, thereby reducing network load and enhancing privacy. Blockchain provides a secure and immutable ledger for recording quality and safety assessments, utilizing Hyperledger for scalability and support for permissioned networks. Smart contracts ensure compliance with safety standards and enable seamless and automated verification of transactions.

The TrustFish framework integrates federated learning and blockchain technologies to establish a decentralized, secure, and efficient system for monitoring seafood quality and safety. Stakeholders can keep an eye on seafood quality [23], thanks to TrustFish's end-to-end traceability. Thus, the TrustFish framework advances the seafood industry's shift to Industry 5.0 by transforming the supply chain into a transparent, effective, and secure system. The end-to-end architecture, which is organized around five stakeholders, is shown in Fig. 1:

- **Fisher:** Operates fishing vessels equipped with IoT sensors to monitor catch, responsible for logging the origin and initial quality conditions of the seafood.
- **Transporter:** oversees vehicles that are refrigerated and have sensors for humidity and temperature. The stakeholder keeps track of environmental aberrations and guarantees the integrity of the cold chain during land and marine transportation.
- **Storage:** Monitoring is for detecting long-term exposure to suboptimal conditions that could lead to spoilage.
- **Shipper:** Seafood distribution to retailers and verifies maintenance of the cold chain during the final leg of logistics.
- **Retailer:** The final point of sale (e.g., supermarkets) display conditions until purchase. The node provides the quality assessment before the product reaches the consumer.

Table 2
Comparative analysis of seafood supply chain and blockchain-federated learning frameworks.

Study	Traceability	Quality	Integration	Advanced Privacy (DP/HE)	Scalability Solution	Seafood Focus
[19]	✓	×	×	×	×	×
[23]	✓	×	×	×	×	✓
[25]	×	✓	×	×	×	×
[6]	×	✓	✓	×	×	×
[28]	×	✓	✓	×	×	×
[27]	×	✓	✓	×	×	×
[29]	×	✓	✓	×	×	×
Our work	✓	✓	✓	✓	✓	✓

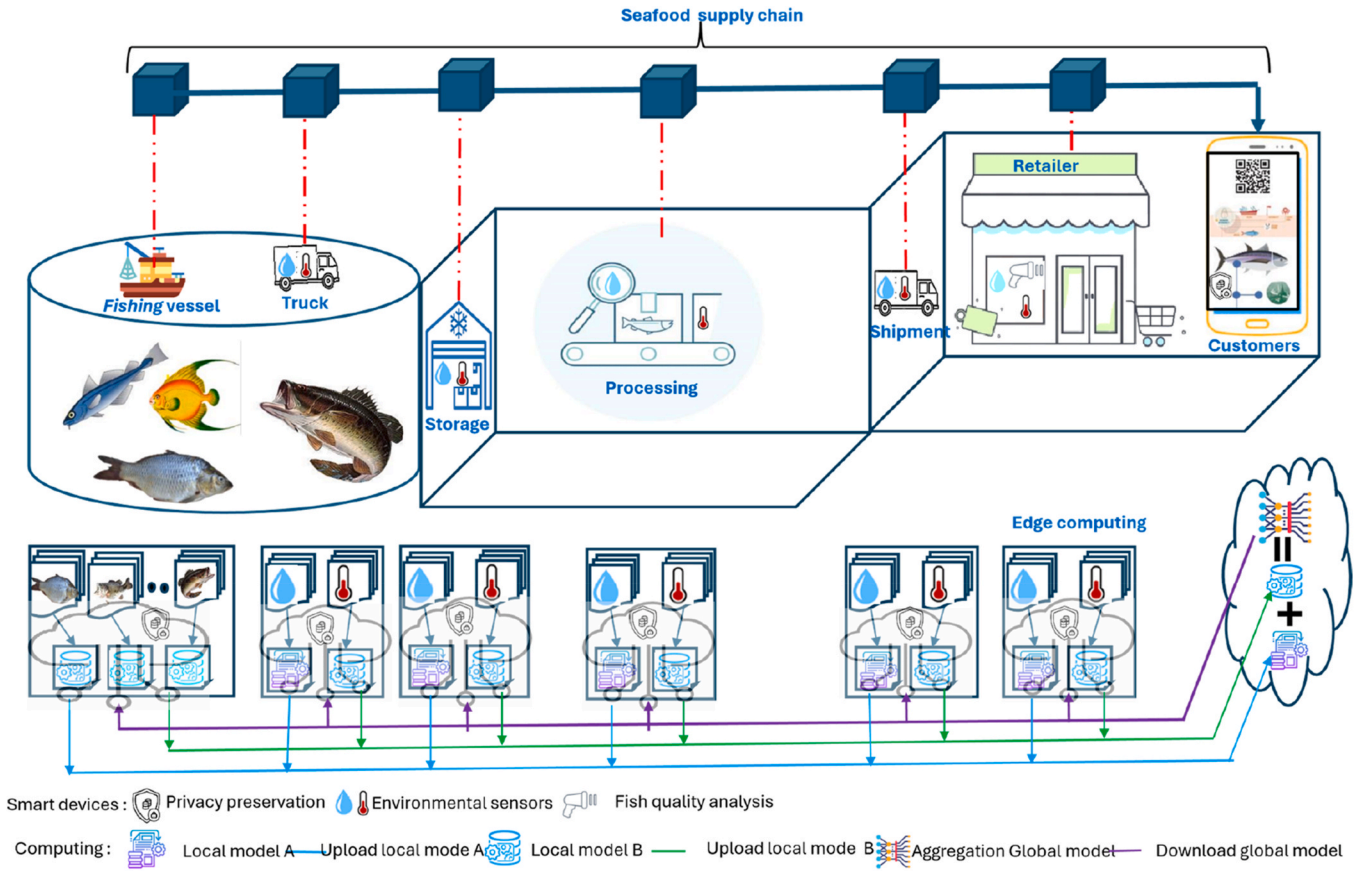

Fig. 1. TrustFish framework.

IoT devices gather real-time data such as temperature and humidity at the seafood supply chain node. A federated learning model is used to process gathered data locally. Stakeholder trains a local model and sends model updates (weights) to a central aggregator rather than sharing raw data, leading to a lower bandwidth consumption and to data privacy protection. Blockchain network built on Hyperledger, runs in parallel. Every quality assessment, model update hash, and significant transaction is immutably recorded on the blockchain. Each stakeholder acts as a node in this permissioned network, enabling them to verify the entire history of a product. Smart contracts automate compliance verification and actions if predefined safety thresholds are breached. The system collective intelligence is increased via central federated learning aggregator to improve a global model. Blockchain offers a reliable, impenetrable record of the whole process, while federated learning offers decentralized intelligence for quality prediction. Customers may build confidence and make educated purchases by using QR codes to obtain clear histories.

3. PROOF-OF concept

We present a robust and secure framework for monitoring seafood quality and safety. The TrustFish integrates data from IoT sensors distributed across various nodes in the supply chain and applies a decentralized, privacy-preserving approach to model training. Blockchin enhances data integrity and traceability, ensuring trustworthiness in traceability and quality monitoring. Through controlled experiments utilizing synthetic data calibrated to industry standards (HACCP, ICMSF), we explicitly validate three aspects: (1) interoperability between federated learning and blockchain modules—demonstrating how model updates are securely hashed and immutably recorded; (2) data flow integrity across the supply chain—from IoT sensor data to local model training, secure aggregation, and blockchain logging; and (3) security properties—validating the tamper-evidence of the blockchain ledger through hash-based verification and the privacy guarantees of our DP-HE approach. The experimental validation confirms that TrustFish components interact to achieve privacy, traceability, and trustworthiness.

3.1. Data collection and preprocessing

The data used in TrustFish framework are generated from synthetic IoT devices placed at different stages of the supply chain (i.e., Fisher, Transporter, Storage, Shipper, and Retailer). Synthetic data simulates realistic spoilage conditions across nodes, providing a preliminary validation environment with thresholds based on industry standards to ensure alignment with real-world conditions. Table III shows a preview with the first few rows of the data. Each node (Fisher, Storage, Retailer, Shipper, and Transporter) collected 100 samples for each quality category, 'Good,' 'Moderate,' and 'Poor,' resulting in a total of 1500 samples across all nodes. Each node N_i captures real-time data on temperature and humidity in the seafood supply chain for quality assurance. The data is formulated as follows:

Table 3
Sample data of seafood quality monitoring across nodes: R=ROW, T = TEMPERATURE, H=HUMIDITY, Q = QUALITY, G = GOOD, M = MODERATE.

R	Timestamp	T	H	Q	Node
1	2024-10-30 17:01:45.318	10.17	69.94	G	Fisher
2	2024-10-28 12:01:45.324	9.41	79.479	G	Storage
3	2024-10-29 04:01:45.327	10.66	72.826	G	Retailer
4	2024-10-30 05:01:45.318	12.989	83.169	M	Shipper
5	2024-10-28 19:01:45.322	13.719	76.27	G	Transporter

$$D_{N_i} = \{(t_j, h_j, q_j)\}_{j=1}^{100}, \quad \forall N_i \in \text{Nodes} \tag{1}$$

Where the temperature and humidity data represents by t and h, respectively. The quality label classifies as *Good*, *Moderate*, and *Poor* indicates by the q. Conditional criteria for humidity and temperature are used in quality labeling to represent actual spoiling conditions. Pre-processing involves encoding quality labels into integers using label encoding and scaling temperature and humidity data to a range of [0,1] with Min-Max scaling:

$$t' = \frac{t - \min(t)}{\max(t) - \min(t)} \tag{2}$$

$$h' = \frac{h - \min(h)}{\max(h) - \min(h)} \tag{3}$$

The steps ensure model consistency between nodes, minimize scaling discrepancies, and improve learning efficiency.

3.2. Dataset Justification and labeling policy

Since publicly available seafood IoT datasets are limited, we generate synthetic sensor data calibrated to industry standards (HACCP and ICMSF). Quality labels follow rule-based thresholds: *Good* if $T \leq 4$ °C and RH$\leq$ 75%, *Moderate* if $4 < T \leq 7$ °C or 75 $<$ RH $\leq$ 85%, and *Poor*-otherwise. These values mirror cold-storage practice for iced finfish. Section V-A discusses dataset bias and our plan to validate our model using real seafood data from industry partners.

3.3. Federated learning framework

Federated learning enables nodes to train a local model on private data. The setup supports collaborative learning, preserves privacy of individual nodes, and communicate model weights. The chosen model includes a three-layer neural network with ReLU activation in hidden layers and Softmax in the output layer. The layer is selected based on tests that showed well-suited for classification task, balancing performance with computational efficiency. Other architectures, such as deeper networks, were considered but found to increase computational demands without significantly improving classification performance, making this three-layer setup an optimal choice for this application.

Each node trains a neural network model with an input vector $X = \{t', h'\}$ and a target label $y = q$. The local model M_i at node N_i learns a mapping f: $X \rightarrow y$. To reduce resource demands at each node, which might have limited bandwidth and processing power, the federated learning framework optimizes model training through Federated Averaging (FedAvg), an aggregation technique that reduces the need for large-scale data transmission by only transmitting model weights. The objective function for each local model minimizes the cross-entropy loss

$$\mathscr{L}(y, \hat{y}) = -\sum_{c=1}^{C} y_c \log(\hat{y}_c) \tag{4}$$

where y_c is the true label for class c and $\hat{y}_c$ is the predicted probability for that class and C is the number of classes.

Algorithm 1. Federated learning with decentralized data

Require: Set of nodes $N = \{N_1, N_2, \ldots, N_k\}$, model architecture M, learning rate η, epochs E
Ensure: Global model M_{global}
1 Initialize global model weights W_{global}
2 **for** each communication round $r = 1, 2, \ldots, R$ **do**
3 **for** each node $N_i \in N$ in parallel **do**
4 Download W_{global} to local model M_i
5 Train M_i on local dataset D_{N_i} for E epochs
6 Upload updated weights W_{N_i} to server
7 **end for**

(*continued on next column*)

(*continued*)

8 Aggregate weights: $W_{global} = \frac{1}{k}\sum_{i=1}^{k} W_{N_i}$
9 **end for**

The central server aggregates the weights W_{N_i} of each node in each communication round to update the global model M_{global}, thus reducing the data transfer load and computational cost while preserving privacy. Federated averaging aggregation provides efficient updates, ensuring that the model is suitable for a distributed environment such as the seafood supply chain.

$$W_{\text{global}}^{(t+1)} = \frac{1}{k}\sum_{i=1}^{k} W_{N_i}^{(t+1)} \tag{5}$$

where k is the number of participating nodes around t and $W_{N_i}^{(t+1)}$ are the local weights after training. Each node clips gradients to norm C and adds Gaussian noise $\mathcal{N}(0, \sigma^2 I)$ according to the moments-accountant budget ε_r (cosine-decay schedule). Optionally, updates are encrypted with CKKS before aggregation. This dual layer—differential privacy plus HE—prevents the aggregator from inferring raw sensor data while maintaining acceptable model utility.

3.4. Blockchain for integrity and traceability

Blockchain is integrated to ensure traceability and prevent tampering with the quality assessments performed in the seafood supply chain. Each block in the blockchain logs quality data from nodes, accompanied by a timestamp, providing an immutable record of seafood quality throughout the supply chain. We employ the Hyperledger architecture for implementation, which is chosen due to robustness in handling blockchain-based data sharing, scalability, and support for permissioned networks, making it ideal for fulfilling supply chain privacy and security needs. To confirm the integrity of every block in the chain, hash-based validation has been included in the blockchain architecture. Each block contains H_{prev} the hash of the previous block, Q_{N_i} the quality data for node N_i, T is timestamp and $\|$ denotes concatenation. The hash for each block is calculated as:

$$H_{\text{block}} = \text{SHA256}\left(H_{\text{prev}} \| Q_{N_i} \| T\right) \tag{6}$$

The method breaks the chain and reveals efforts at tampering by guaranteeing that Q_{N_i} or T modifies H_{block}. Hyperledger facilitates safe data exchange in the supply chain by controlling chain integrity to support TrustFish architecture. In order to ensure that stakeholders have faith in the integrity of the seafood quality monitoring process, TrustFish offers safe, traceable records of seafood quality evaluations.

Algorithm 2. Blockchain for secure data logging

Require: Quality data Q_{N_i} from node N_i, previous hash H_{prev}
Ensure: Append block to blockchain
1 Compute timestamp $T \leftarrow$current time
2 Create block content $C \leftarrow H_{\text{prev}} \| Q_{N_i} \| T$
3 Calculate hash $H_{\text{block}} = \text{SHA256}(C)$
4 Append block $B \leftarrow \{H_{\text{prev}}, Q_{N_i}, H_{\text{block}}, T\}$ to blockchain

3.5. Dynamic sharding and directed acyclic graph consensus

Nodes are grouped to enhance scalability by supply-chain stage into dynamic shards. Within each shard, events form directed acyclic graph enabling parallel block confirmation. Checkpoints sign by shard leaders are reconciled by the ordering service, reducing cross-node latency and improving throughput. The network is partitioned into k shards. k is adjusted based on the network load and active nodes. Shard assignment for a node N_i is determined by a verifiable random function. Verifiable

random function considers the node's stake, historical reliability, and current shard load to ensure balanced distribution and mitigate attacks:

$$\text{ShardID}(N_i) = \text{VRF}(\text{PK}_{N_i}, \text{Stake}_{N_i}, \text{Load}_{\text{shard}}) \bmod k \tag{7}$$

3.6. Privacy-preserving mechanism with differential privacy and HE

To ensure a robust privacy without sacrificing the model utility, TrustFish employs a layered approach combining DP and HE, drawing on established privacy-preserving federated learning [7,29]. Before uploading model updates, each client node adds calibrated noise to its local model gradients. We use the Gaussian mechanism for continuous data. For a given privacy budget ϵ and sensitivity Δ, the noise scale σ is calculated as:

$$\sigma = \frac{\Delta\sqrt{2\ln(1.25/\delta)}}{\epsilon} \tag{8}$$

where δ is a small probability of privacy loss exceeding ϵ. The sensitivity Δ is bounded by gradient clipping. We empirically set $\epsilon = 1.0$ and $\delta = 10^{-5}$ for our experiments, a configuration that provides a strong privacy guarantee while maintaining model accuracy, as validated in Ref. [29].

To prevent the central aggregator from accessing plaintext model updates, even after noise addition, we employ the Paillier cryptosystem, an additive HE scheme.

$$C_{N_i} = \mathscr{E}_{\text{PK}}(\widetilde{W}_{N_i}) \tag{9}$$

The aggregator then performs a secure aggregation on the ciphertexts:

$$C_{\text{global}} = \bigoplus_{i=1}^{k} C_{N_i} = \mathscr{E}_{\text{PK}}\left(\sum_{i=1}^{k} \widetilde{W}_{N_i}\right) \tag{10}$$

Where $\mathscr{E}_{\text{PK}}(\cdot)$ denotes encryption under public key *PK*, and $\oplus$ denotes the homomorphic addition operation on ciphertexts.

The resulting ciphertext C_{global} is decrypted only by a designated consensus of nodes (or via a threshold decryption scheme) to obtain the aggregated global model update.

3.7. Communication and systems cost

Let P be the model parameters (bytes b each), k clients, and R rounds. The total uplink traffic is $k \cdot P \cdot b \cdot \alpha$, where α is the encryption expansion factor. Fabric endorsement and ordering latencies average 1–2 s per block; the total storage growth during simulation was 10 MB for 1500 transactions. These measurements confirm feasibility for near-real-time seafood monitoring.

3.8. Data analysis and visualization

We track the temperature and the humidity in time for supply chain nodes to analyze environmental trends. The metrics are aggregated by node and quality level to reveal correlations and visualize node distribution patterns.

3.8.1. Temperature and humidity analysis

The average temperature and humidity for each quality class are computed by node:

$$\text{Avg. Temperature} = \frac{1}{n}\sum_{j=1}^{n} t_j \tag{11}$$

$$\text{Avg. Humidity} = \frac{1}{n}\sum_{j=1}^{n} h_j \tag{12}$$

3.8.2. Quality level distribution

'Good,' 'Moderate,' and 'Poor' are the quality level distribution in the seafood supply chain that are shown by bar plots and scatter plots. The visualizations show the impact of environmental conditions on the seafood quality, providing actionable insights for targeted interventions.

3.9. Comparison with centralized baseline

We validate the federated learning model using benchmark comparisons with a centralized Random Forest model trained on aggregated data, which provides a basis for evaluating the decentralized approach. We use a centralized Random Forest (RF) model trained on the full aggregated dataset as a performance upper-bound to put our decentralized federated learning approach's performance in perspective. The accuracy of the centralized RF model acheives 91%. The substantial benefits provided by our TrustFish architecture make the minor performance disparity (4%) an attractive trade-off. The federated learning approach eliminates the bandwidth expense of centralizing raw sensor data, maintains data privacy by design, and aligns well with the supply chain's decentralized structure. The findings demonstrate that near-optimal monitoring accuracy can be achieved without compromising the core principles of data security and sovereignty. The Random Forest model is hyperparameter-tuned using GridSearchCV with the following settings:

$$\text{Parameters} = \left\{ \begin{array}{l} \text{n\_estimators} \in \{100, 200, 500\}, \\ \text{max\_depth} \in \{10, 20, \text{None}\}, \\ \ldots \end{array} \right\} \tag{13}$$

The model is evaluated with accuracy, precision, recall, and F1-score, computed as follows:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{14}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{15}$$

$$\text{F1} - \text{score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{16}$$

Where TP, TP, FP,FP, and FN denote true positives, false positives, and false negatives, respectively. The metrics comprehensively evaluate the model's performance for quality classification.

4. Experimental results and discussion

The results demonstrate TrustFish's effectiveness in the seafood supply chain. Figs. 2 and 3 show temperature trends in the seafood supply chain, emphasizing how temperature changes happen all throughout the supply chain and how they affect the seafood quality.

4.1. Analysis of environmental trends and spoilage correlations

Fig. 6 offers deeper insight into the relationships between environmental conditions and seafood quality by showing average temperature and humidity by quality level and node. A critical analysis of the environmental data, summarized in Fig. 6, reveals clear and actionable correlations between storage conditions and seafood quality. Samples classifies as 'Poor' quality in the storage node are associated with an average humidity of 85% ± 5% and a temperature of 6.5 °C ± 1.5 °C. In contrast, 'Good' quality samples in the same node are maintained at a significantly lower average humidity of 70% ± 3% and a tighter temperature range of 3.2 °C ± 0.5 °C. In the results, nodes in supply chain such as storage and retailers have greater humidity swings, which frequently correspond to samples of "poor" quality. These nodes could need more stringent environmental management.

The Transporter node exhibited the most considerable temperature

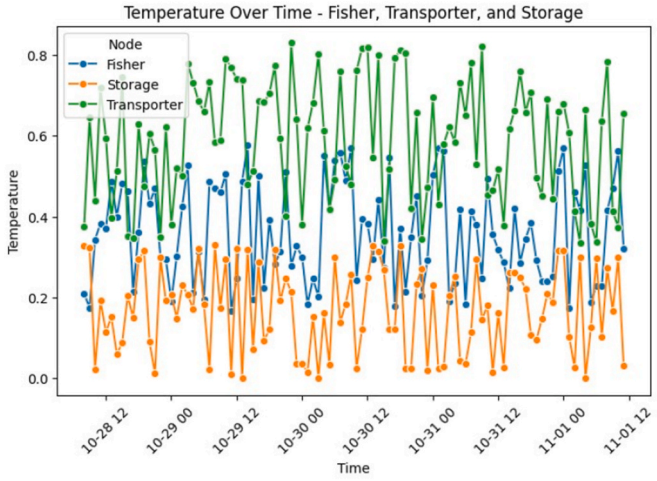

Fig. 2. Temperature in seafood supply chain, including fisher, transporter, and storage.

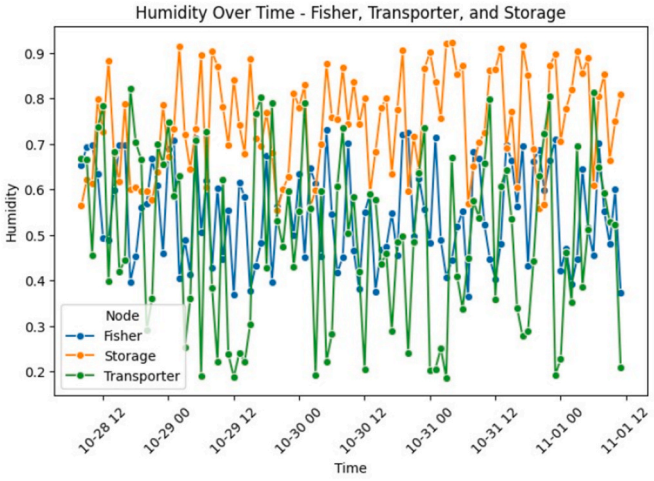

Fig. 4. Humidity in seafood supply chain, including fisher, transporter, and storage.

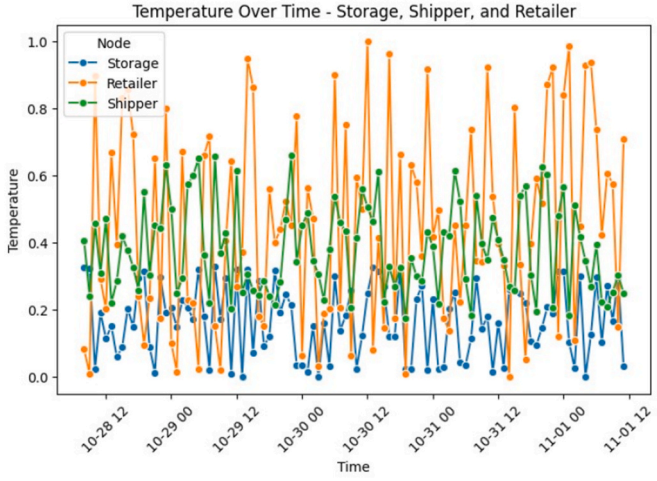

Fig. 3. Temperature in seafood supply chain, including storage, shipper, and retailer.

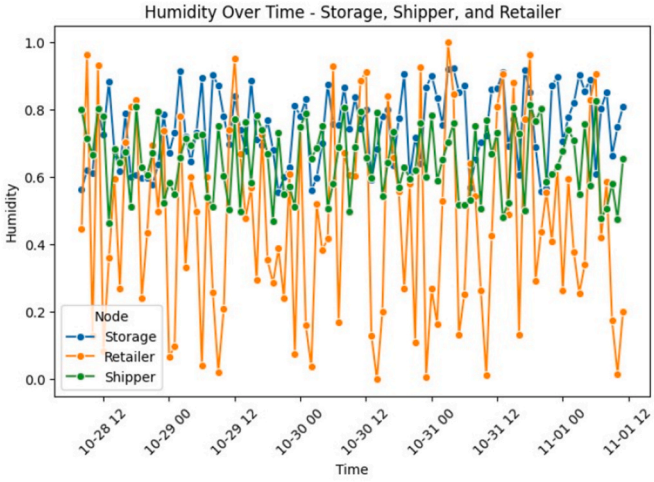

Fig. 5. Humidity in seafood supply chain, including storage, shipper, and retailer.

volatility, with values ranging from 2 °C to 10 °C. The highest rate of quality degradation in the chain, with 40% of samples classified as "Moderate" or "Poor," is correlated with instability. The results identify the transporter and storage phases as control points. When criteria are crossed (for example, humidity > 80% in storage), the TrustFish's real-time monitoring may set out automatic alarms, allowing for preventative measures to stop spoiling before it starts. Figs. 4 and 5 show humidity trends in the same nodes are critical to determining quality. Figs. 4 and 5 show how temperature and humidity fluctuate in the seafood supply chain.

4.2. Blockchain performance and data integrity validation

Blockchain implemented in TrustFish provides a transparent and tamper-proof mechanism, utilizing hash-based validation to ensure data integrity in the seafood supply chain. By leveraging Hyperledger to create a permissioned blockchain environment, we enhance the supply chain trust by providing a secure access to high-quality data. Because the integrity of quality monitoring in the recorded data would be compromised, the arrangement shows that tampering would be evident. The configuration demonstrates that manipulation would be blatant, as the integrity of quality monitoring in the recorded data would be disrupted. The Hyperledger blockchain backbone recorded all model updates and quality assessments. The system's viability for near-real-time monitoring is confirmed by the experiment, which involves 1500 transactions and achieves an average latency of 1.5 s. To verify the hash-based validation (Eq. (5)), one must (i) try to change a recorded quality score after the fact; (ii) have any changes instantly invalidated; and (iii) provide the promised tamper-evidence. It offers a degree of confidence for the TrustFish system.

4.3. Quantitative classification results

Federated learning classification performance is visualized in the confusion matrix as shown in Fig. 7. The matrix illustrates the accuracy of federated learning in classifying data into the "Good," "Moderate," and "Poor" categories, as well as instances of misclassification between adjacent quality categories. The errors occur due to borderline temperature and humidity values that overlap with quality thresholds, indicating areas where the model's decision boundaries require improvement. The performance of the federated learning model was rigorously evaluated on a held-out test set. Table III illustrates the model's effectiveness in classifying seafood quality in the supply chain. The model achieves overall accuracy of 87%, as shown in Table IV. Fig. 7) shows examination of the confusion matrix. The high F1-scores for 'Good' (0.90) and 'Poor' (0.92) classes indicate the model is highly

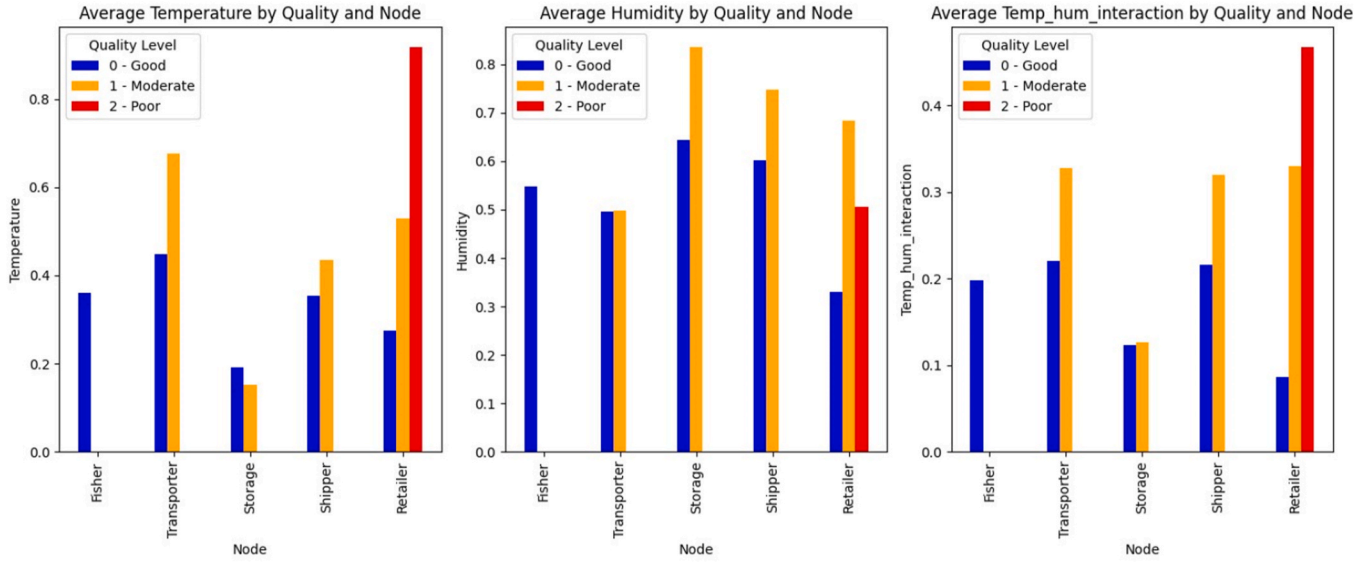

Fig. 6. Average temperature and humidity in seafood quality across supply chain.

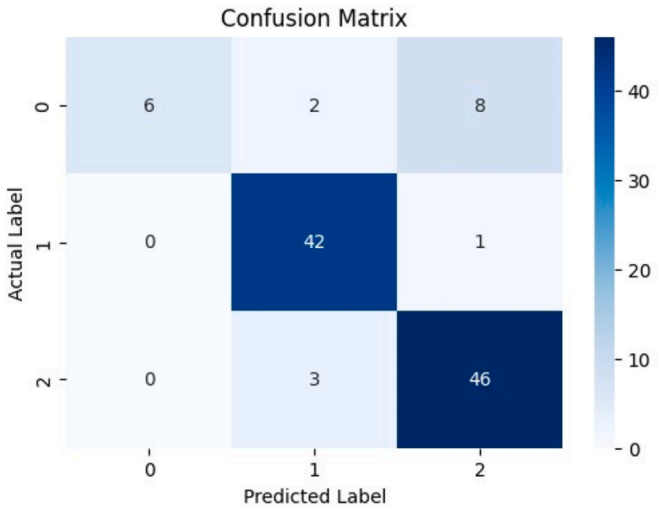

Fig. 7. Confusion matrix on test set.

Table 4
Federated learning model performance.

Quality Class	Precision	Recall	F1-Score	Support
Good	0.92	0.88	0.90	150
Moderate	0.81	0.75	0.78	150
Poor	0.94	0.91	0.92	150
Accuracy			0.87	450
Macro Avg	0.89	0.85	0.87	450

reliable at identifying clear cases of freshness and spoilage. The challenge lies in the 'Moderate' class (F1-score: 0.78), where 40 samples are misclassified—15 as 'Good' and 25 as 'Poor'. It is expected, as the environmental conditions (e.g., temperature between 5 and 7 °C) defining the 'Moderate' class inherently create a transitional zone that overlaps with the thresholds of the neighboring classes (see Table 5).

The accuracy of the federated learning model in predicting fish quality is shown in Fig. 8. Fig. 8 provide a comparison between the model predictions and the ground truth labels. The model's classification efficacy is demonstrated by the predictions matching the actual quality labels. Fig. 8 illustrates how the federated learning model forecasts

Table 5
List of abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
BFT	Byzantine Fault Tolerance
CPU	Central Processing Unit
IoT	Internet of Things
ML	Machine Learning
PK	Public Key
RF	Random Forest
RFID	Radio-Frequency Identification
ReLU	Rectified Linear Unit
SHA256	Secure Hash Algorithm 256-bit
TruFLaaS	Trustworthy Federated Learning as a Service

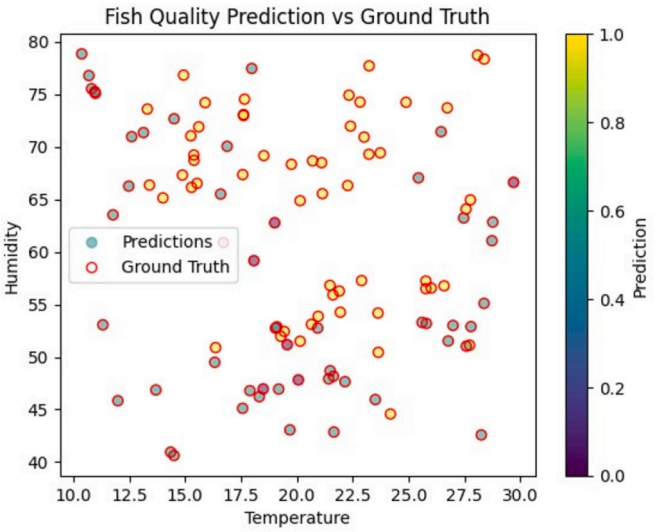

Fig. 8. Fish Quality Prediction vs Ground Truth.

quality and offers improvement to handle intricate environmental interactions. TrustFish shows how to use decentralized data processing to monitor seafood quality. For monitoring seafood quality, TrustFish provides a privacy-preserving approach and guaranteeing data integrity. Moreover, tailored interventions to enhance the overall quality control

throughout the supply chain are made possible by monitoring node-specific environmental conditions.

4.4. Synthesis and practical implications

TrustFish creates a synergistic loop for quality assurance. A Federated learning model provides intelligent, localized into quality degradation, while the blockchain provides an immutable, trusted record of these assessments. When a federated learning model at a Retailer node predicts a transition from 'Good' to 'Moderate' quality, this event, along with the relevant temperature/humidity data, is immutably logged on the blockchain. This provides a verifiable and tamper-proof audit trail for all stakeholders. A consumer scans a product QR code to access the seafood's history in the seafood supply chain, fostering unprecedented transparency and trust. For a regulator, the proposed system enables rapid and accurate root-cause analysis in the event of a contamination incident, dramatically reducing the investigation time.

4.5. Blockchain performance and security evaluation

Hyperledger Fabric network (2 organizations, 3 peers each, Raft ordering) process 1500 transactions with average endorsement latency 1.4 s and throughput 25 tx/s. Post-hoc tampering tests invalidated hash links as expected, confirming data immutability. Because Fabric is permissioned, no gas costs apply; resource usage was low ($\leq$8 % CPU per peer).

5. Limitations and future work

This section focuses on the discussion of the limitations and future work.

5.1. Limitations

TrustFish framework demonstrates significant potential for enhancing seafood supply chain monitoring, but there are some limitations to be presented as potential opportunities for future research.

- **Synthetic data:** Data is generated to reflect realistic industry thresholds. Data generated may not capture factors (i.e., noise, outliers, and complex), non-linear spoilage dynamics of a real-world operational environment.
- **Environmental parameters:** There are factors (i.e., shock/vibration, atmospheric gas composition, and pH levels) can impact the quality of seafood products.
- **Scalability and performance:** the integrated blockchain-federated learning system is evaluated on a limited scale. However, deploying TrustFish framework's behavior, multi-regional supply chain with thousands of nodes and higher transaction volumes remains to be tested.

5.2. Future work

This subsection focuses on addressing the limitations through the following directions:

- **Deployment and validation:** We plan to collaborate with industry partners to deploy the TrustFish framework in a live supply chain. It will allow us to validate TrustFish performance with real IoT data and refine the model under actual operational constraints.
- **Fusion of multi-modal sensor data:** Data from a greater variety of sensors (such as pH meters, gas sensors, and accelerometers) will be included in subsequent generations. The information will allow for a comprehensive and precise evaluation of the product's quality.
- **Large-scale scalability and optimization:** The computation overhead, communication costs, and transactions of TrustFish, as well as the heterogeneous network, will be thoroughly examined. We will explore optimal sharding algorithms and lightweight consensus strategies to enhance scalability.
- **Refined Privacy-utility trade-off:** We will perform quantitative analysis of the trade-off between the privacy budget (ϵ) in DP, aiming to establish privacy parameters for this specific application domain.
- **Deployment and industry validation:** TrustFish deployment in collaboration with seafood industry partners involve: (1) deploying the TrustFish framework on a private Hyperledger Fabric network with actual stakeholder nodes; (2) integrating real IoT sensors and devices for data collection; (3) executing the complete workflow—from data collection through federated learning training to blockchain recording—in a live supply chain segment; and (4) evaluating the system's performance, usability, and business impact.

6. Conclusion

This paper proposed a novel TrustFish framework that combines cutting-edge systems, namely federated learning and blockchain, to address seafood supply chain challenges, supported by a secure and trustworthy management platform. The TrustFish framework has been implemented to manage data and provide information about transactions between supply chains and external parties, such as regulatory authorities. By gathering information from the seafood supply chain and considering related financial risks, smart IoT devices monitor the safety and quality of seafood. In addition to lowering contamination, waste, and seafood fraud, TrustFish guaranteed privacy-preserving data exchange and trust management. TrustFish has enhanced the seafood industry and improved public health by ensuring the delivery of safe, high-quality seafood to consumers.

CRediT authorship contribution statement

Saeed Hamood Alsamhi: Writing – review & editing, Writing – original draft, Supervision, Methodology, Funding acquisition, Conceptualization. **Raushan Myrzashova:** Software, Resources, Methodology, Formal analysis, Data curation. **Ammar Hawbani:** Writing – original draft, Supervision, Data curation. **Mohammed A.A. Al-qaness:** Software, Resources, Project administration. **Xi Wei:** Formal analysis, Data curation. **Liang Zhao:** Investigation, Funding acquisition. **Mohsen Guizani:** Writing – review & editing, Supervision, Formal analysis, Data curation. **Edward Curry:** Visualization, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is supported by project Insight II, "Leveraging Dataspaces for Seafood Sustainability". Furthermore, this publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number SFI/12/RC/2289_P2 and SMACC+ Sustainable Microalgae and Cyanobacteria-Based Bioactive Compounds for Cosmeceuticals and NutraceuticalsInterreg Atlantic Area: EAPA_0145/2024.

Data availability

The authors do not have permission to share data.

References

[1] Amaya Vega, Ana Corina Miller, Cathal O'Donoghue, Economic impacts of seafood production growth targets in Ireland, Mar. Pol. 47 (2014) 39–45.

[2] Zarul Hazrin Hashim, Mohamad N. Azra, Mohd Iqbal Mohd Noor, Nor Azman Kasan, Shau Hwai Tan, Impact of covid-19 on marine fisheries supply chains: case study of Malaysia, in: Advances in Food Security and Sustainability, vol. 6, Elsevier, 2021, pp. 169–210.

[3] Mohammed Ziaul Hoque, Nazmoon Akhter, Mohammad Shafiur Rahman Chowdhury, Consumers' preferences for the traceability information of seafood safety, Foods 11 (12) (2022) 1675.

[4] Xinxin Wang, Yamine Bouzembrak, A.G.J.M. Oude Lansink, H.J. Van Der Fels-Klerx, Application of machine learning to the monitoring and prediction of food safety: a review, Compr. Rev. Food Sci. Food Saf. 21 (1) (2022) 416–434.

[5] Bin Yu, Ping Zhan, Ming Lei, Fang Zhou, Peng Wang, Food quality monitoring system based on smart contracts and evaluation models, IEEE Access 8 (2020) 12479–12490.

[6] Hajar Moudoud, Soumaya Cherkaoui, Lyes Khoukhi, Towards a scalable and trustworthy blockchain: iot use case, in: ICC 2021-IEEE International Conference on Communications, IEEE, 2021, pp. 1–6.

[7] Yanli Ren, Yerong Li, Guorui Feng, Xinpeng Zhang, Privacy-enhanced and verification-traceable aggregation for federated learning, IEEE Internet Things J. 9 (24) (2022) 24933–24948.

[8] Konstantinos Demestichas, Nikolaos Peppes, Theodoros Alexakis, Evgenia Adamopoulou, Blockchain in agriculture traceability systems: a review, Appl. Sci. 10 (12) (2020) 4113.

[9] Carl HB. Haukås, Preconditions to Start and Scale Digital Ecosystems: a Study of Aquacloud in the Norwegian Seafood Industry, 2020. Master's thesis.

[10] Shereen Ismail, Hassan Reza, Khouloud Salameh, Hossein Kashani Zadeh, Fartash Vasefi, Toward an intelligent blockchain iot-enabled fish supply chain: a review and conceptual framework, Sensors 23 (11) (2023) 5136.

[11] I.G. Gleadall, A. Barkai, Z. Lajbner, P.B. McIntyre, H. Moustahfid, P. Olsen, R. Oyanedel, Y. Pang, Graham J. Pierce, L. Quesada, et al., Sustainable seafood: advances in traceability, assessment, monitoring and resource management, Afr. J. Mar. Sci. 46 (4) (2024) 239–245.

[12] Thomas A. Hemphill, Phil Longstreet, Syagnik Banerjee, Automotive repairs, data accessibility, and privacy and security challenges: a stakeholder analysis and proposed policy solutions, Technol. Soc. 71 (2022) 102090.

[13] Brent R. Heard, Morteza Taiebat, Ming Xu, Shelie A. Miller, Sustainability implications of connected and autonomous vehicles for the food supply chain, Resour. Conserv. Recycl. 128 (2018) 22–24.

[14] Huaqun Guo, Xingjie Yu, A survey on blockchain technology and its security, BLOCK: research and applications 3 (2) (2022) 100067.

[15] Saeed Hamood Alsamhi, Raushan Myrzashova, Hawbani Ammar, Santosh Kumar, Sumit Srivastava, Liang Zhao, Xi Wei, Mohsen Guizan, Edward Curry, Federated learning meets blockchain in decentralized data-sharing: Healthcare use case, IEEE Internet Things J. 11 (11) (2024).

[16] Jara Laso, Israel Ruiz-Salmón, María Margallo, Pedro Villanueva-Rey, Lucía Poceiro, Paula Quinteiro, Ana Cláudia Dias, Cheila Almeida, António Marques, Eduardo Entrena-Barbero, et al., Achieving sustainability of the seafood sector in the european atlantic area by addressing eco-social challenges: the neptunus project, Sustainability 14 (5) (2022) 3054.

[17] Deborah M. Power, Petros Taoukis, Dimitra Houhoula, Theofania Tsironi, Emmanouil Flemetakis, Integrating omics technologies for improved quality and safety of seafood products, Aquaculture and Fisheries 8 (4) (2023) 457–462.

[18] Yi-Chih Yang, Han-Yu Lin, Cold supply chain of longline tuna and transport choice, Maritime Business Review 2 (4) (2017) 349–366.

[19] Juan F. Galvez, Juan C. Mejuto, Jesus Simal-Gandara, Future challenges on the use of blockchain for food traceability analysis, TrAC, Trends Anal. Chem. 107 (2018) 222–232.

[20] I. Afrianto, T. Djatna, Y. Arkeman, I. Hermadi, I.S. Sitanggang, Block chain technology architecture for supply chain traceability of fisheries products in Indonesia: future challenge, J. Eng. Sci. Technol. 15 (2020) 41–49.

[21] Shereen Ismail, Muhammad Nouman, Hassan Reza, Fartash Vasefi, Kashani Zadeh Hossein, A blockchain-based fish supply chain framework for maintaining fish quality and authenticity, IEEE Transactions on Services Computing 17 (5) (2024) 1877–1886.

[22] M. Veena, K. Sravani, K. Dhanapal, G. Praveen Kumar, C. Manaswini, D Chand Basha, Blockchain technology for enhancing traceability and sustainability in fish and fishery products: comprehensive review, International Journal of Bio-Resource & Stress Management 16 (9) (2025).

[23] Pratyush Kumar Patro, Raja Jayaraman, Khaled Salah, Ibrar Yaqoob, Blockchain-based traceability for the fishery supply chain, IEEE Access 10 (2022) 81134–81154.

[24] Bahareh Mosadegh Sedghy, Evolution of Radio Frequency Identification (Rfid) in Agricultural Cold Chain Monitoring: a Literature Review, 2018.

[25] Hajar Moudoud, Soumaya Cherkaoui, Lyes Khoukhi, Towards a secure and reliable federated learning using blockchain, in: 2021 IEEE Global Communications Conference (GLOBECOM), IEEE, 2021, pp. 1–6.

[26] Zakaria Abou El Houda, Abdelhakim Hafid, Lyes Khoukhi, Brainchain-a machine learning approach for protecting blockchain applications using sdn, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–6.

[27] Carlo Mazzocca, Nicolò Romandini, Matteo Mendula, Rebecca Montanari, Paolo Bellavista Truflaas, Trustworthy federated learning as a service, IEEE Internet Things J. 10 (24) (2023) 21266–21281.

[28] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, Weiqi Luo, Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive, IEEE Trans. Dependable Secure Comput. 18 (5) (2019) 2438–2455.

[29] Youyang Qu, Longxiang Gao, Tom H. Luan, Yong Xiang, Shui Yu, Li Bai, Gavin Zheng, Decentralized privacy using blockchain-enabled federated learning in fog computing, IEEE Internet Things J. 7 (6) (2020) 5171–5183.

[30] Lei Feng, Yiqi Zhao, Shaoyong Guo, Xuesong Qiu, Wenjing Li, Peng Yu, Blockchain-based asynchronous federated learning for internet of things, IEEE Trans. Comput. 99 (1) (2021) 1–9.

[31] Prince Jebedass Isaac Chandran, S Hana Ahmed Khalil, P.K. Hashir, et al., Smart technologies in aquaculture: an integrated iot, ai, and blockchain framework for sustainable growth, Aquac. Eng. (2025) 102584.

[32] Safa Otoum, Ismaeel Al Ridhawi, Hussein T. Mouftah, Blockchain-supported federated learning for trustworthy vehicular networks, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.

[33] Haohan Ding, Wenxu Cheng, Xiaodong Song, Guanjun Dong, Xiaohui Cui, Wei Yu, David I. Wilson, Integration of distributed technologies for intelligent food quality and safety management: blockchain, iot, and federated learning, Food Rev. Int. (2025) 1–23.

[34] Xavi Masip-Bruin, Eva Marín-Tordera, José Ruiz, Admela Jukan, Panagiotis Trakadas, Ales Cernivec, Antonio Lioy, Diego López, Henrique Santos, Antonis Gonos, et al., Cybersecurity in ict supply chains: key challenges and a relevant architecture, Sensors 21 (18) (2021) 6057.

[35] Martí Miquel Martínez, Eva Marin-Tordera, Xavi Masip-Bruin, Scalability analysis of a blockchain-based security strategy for complex iot systems, in: 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), IEEE, 2021, pp. 1–6.

[36] Konstantinos Demertzis, Lazaros Iliadis, Elias Pimenidis, Nikolaos Tziritas, Maria Koziri, Panagiotis Kikiras, Michael Tonkin, Federated blockchained supply chain management: a cybersecurity and privacy framework, in: Artificial Intelligence Applications and Innovations: 17Th IFIP WG 12.5 International Conference, AIAI 2021, Hersonissos, Crete, Greece, June 25–27, 2021, Proceedings 17, Springer, 2021, pp. 769–779.

[37] Zhilin Wang, Qin Hu, Blockchain-based federated learning: a comprehensive survey, arXiv preprint arXiv:2110.02182 (2021). https://doi.org/10.48550/arXiv.2403.19178.