UFT Academic Publishing House, Plovdiv

Food Science and Applied Biotechnology
e-ISSN: 2603-3380

Special Issue: AI and Big Data Analytics for Sustainable Crop and Food Productivity

Journal home page: www.ijfsab.com

CC BY SA

OPEN ACCESS

Research Article

Blockchain data integrity in agri-food system policy implications and ethics in AI driven agriculture

Kamatchi Sundravadivelu[1]✉, Shanmuga Sundar Suruthi[2], Anbazhagan Vijay[3], Selvaraj Karthika[4]

[1]*School of Information Technology, Madurai Kamaraj University, Madurai, Tamil Nadu, India*
[2]*Department of Electronics and communication Engineering, Easwari Engineering College, Tamil Nadu, India*
[3]*Department of Electronics and Communication Engineering, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India*
[4]*Department of Artificial Intelligence and Machine Learning, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India*

Abstract

The blockchain is a decentralized and resistant to tampering ledger system that ensures transparency, immutability and trust within distributed networks, which makes it an efficient mechanism of securing EPCIS supply-chain data. Artificial Intelligence (AI) augments this area enabling predictive analytics, anomaly detection and automated decision-making of large-scale supply-chain event logs. To overcome such difficulties, the workflow suggested includes a number of innovative AI-based elements. Original Graph Neural Networks (GNNs) model EPCIS Object, aggregate, and transaction event logs to reveal product movement channel relational and temporal correlations. Federated Blockchain Integrity Learning (FBIL) validates local data on distributed nodes using blockchain consensus for tamper-resistant, reliable data. To improve detection rates, Deep Reinforcement Learning-Enhanced Logistic Regression (DRL-LR) reinforces model parameters with verified data and rewards. ERPM determines fairness, transparency, compliance, and ethical impact by mapping predictions to any policy norm. Quantum-Inspired Blockchain Security (QIBS) secures crucial EPCIS data using qubits and quantum-like probabilistic transformations. Every encrypted event is verified using HMAC. This combination produces safe, ethical, interpretable, and reliable AI-informed supply-chain intelligence.

Keywords

blockchain data integrity, AI-driven agriculture, EPCIS dataset, supply chain traceability, agri-food systems, data ethics, secure IoT, predictive analytics, policy compliance

Abbreviation

AI – artificial intelligence; ERPM – ethical risk prediction model; FCAI – farmer-centered; AI framework IoT – internet of things.

Corresponding author: *Dr. K. Sundravadivelu, Assistant Professor of Computer Science, School of Information Technology, Madurai Kamaraj University, Madurai, Tamil Nadu, India, Mail: svadivelu2021@gmail.com*

Article history:
Received 28 November 2025
Reviewed 21 April 2026
Accepted 20 May 2026
Available on-line 15 June 2026

2026, UFT Academic publishing house, Plovdiv

PROOF

Introduction

The agri-food system is a series of interlinked processes that ensure the production, processing, transport, and consumption of food in a safe and sustainable manner due to food quality and safety concerns throughout numerous international supply chains. Digital transformation in the agricultural sector is accompanied by a number of policy concerns regarding the transparency, accountability, and ethical use of data to preserve farmers' rights and equitability. Digital platforms should foster the retention of farmer trust. Digital platforms should foster the retention of farmer trust (Ayorinde et al. 2025). Policymakers should devise secure data exchange, algorithmic fairness and responsible use of technology to mitigate the vulnerabilities of food piracy, supply chain disruption and misuse of data from the agricultural sector that is sensitive in nature. Since certain rural communities or small-scale farmers tend to be disadvantaged, the ethical concerns particularly regarding data ownership, informed consent, and algorithmic bias are of concern. The extension of trust, traceability, and immutability within agri-food networks has been and remains a potential with blockchain technology. Improved stakeholder collaboration, prevention of data tampering, and secured transaction within rural and agricultural environments have collaboratively been identified within the research (Azfaralariff et al. 2025). Improved transparency and efficient transaction of data, particularly within agricultural ecosystems are seen within hybrid blockchain–AI frameworks (Aggarwal et al. 2024). Potential drawbacks of blockchain such as limited scalability, latency, high energy consumption, and rural infrastructure integration complexities should be addressed. These limitations restrict its large-scale deployment in low-resource agri-food environments. Predictive analytics, decision execution, and real-time anomaly detection functions across the agri-food supply chain are augmented by Artificial Intelligence (AI). AI-enabled secure frameworks have shown promising potential for addressing cyber risks and facilitating automation within the agricultural Internet of Things (Alharbi et al. 2025). Contrarily, the AI features of data biases, lack of explainability, and susceptibility to adversarial attacks could erode trust and reliability into agricultural decision systems (Bandara et al. 2024). There are ethical implications with AI decision-making impacting farmers' livelihoods, and no adequate explanation provided. Latitude to Implementing Technology and Ethics Based on Bias, Poor Explainability and Vulnerability to Adversarial Attacks, More Recent Works Have Provided Integrated Models of AI, Blockchain, Cryptography, and the Internet of Things as Developing Single, Seamless, and Secure Digital Ecosystems (Bewong et al. 2023). Consistent with these improvements, my methodology utilizes advanced encryption, AI anomaly detection systems, and blockchain for integrity verification to address the remaining gaps. This combined method mitigates the blockchain load through lightweight hashing, employs behavior-based learning models to improve AI reliability, and ensures ethical and policy-aligned data governance (Brummer et al. 2024). The advanced system offers a resilient, transparent, and trustworthy agri-food ecosystem, Security Instruments Digital Agriculture, and Sustainable Agriculture Fig. 1 show that the entire workflow for the smart and secure supervision of the food supply chains. The food supply chains begin with the entry of the data collated and sourced from the various supply chains. The steps of the workflow ensures that the relevant EPCIS events and transactional data are processed and captured for acquisition by the dataset module. The data is then processed for data integrity verification, in which FBIL as a method for integrity verification of federated blockchains is then data processed. After verification, the dataset moves on to data analytics, prediction and forecasting, in which the AI-driven Graph Neural Networks and Deep Reinforcement Learning–Enhanced Logistic Regression models analyze the events, then provide predictive and measurable action and risk forecasts as well as the identification of the events of the system for aberrant activity. The results are then measured through the impact of policies on the metrics of evaluation of ethics and models of Enterprise Resource Project Management with the assurance of equity, compliance, and transparency of the decision as. At the same time, the system with the Quantum-Inspired Blockchain Security and HMAC protects data from tampering and unauthorized access. Subsequently, the system provides the overall data security. The system provides a reliable and ethically governed supply chain intelligence

PROOF

system that uses blockchain and AI and is integrated.

Cybersecurity breaches have claimed a variety of impacts, such as loss of data, loss of efficiency from digitized systems, and loss of food security. A key mitigation strategy against cybersecurity threats is the deployment of advanced technologies such as Artificial Intelligence (AI), Blockchain, and Quantum Computing to enhance malware detection in Internet of Things (IoT) digital devices and provide prompt threat response (Dzreke et al. 2025). Notably, the infrastructures of rural areas to enable smallholder farmers to take advantage of the adoption of AI and Blockchain remains a concern. Blockchain technology preserves trust among participants like farmers, distributors, retailers, and consumers, as data records are unchangeable.

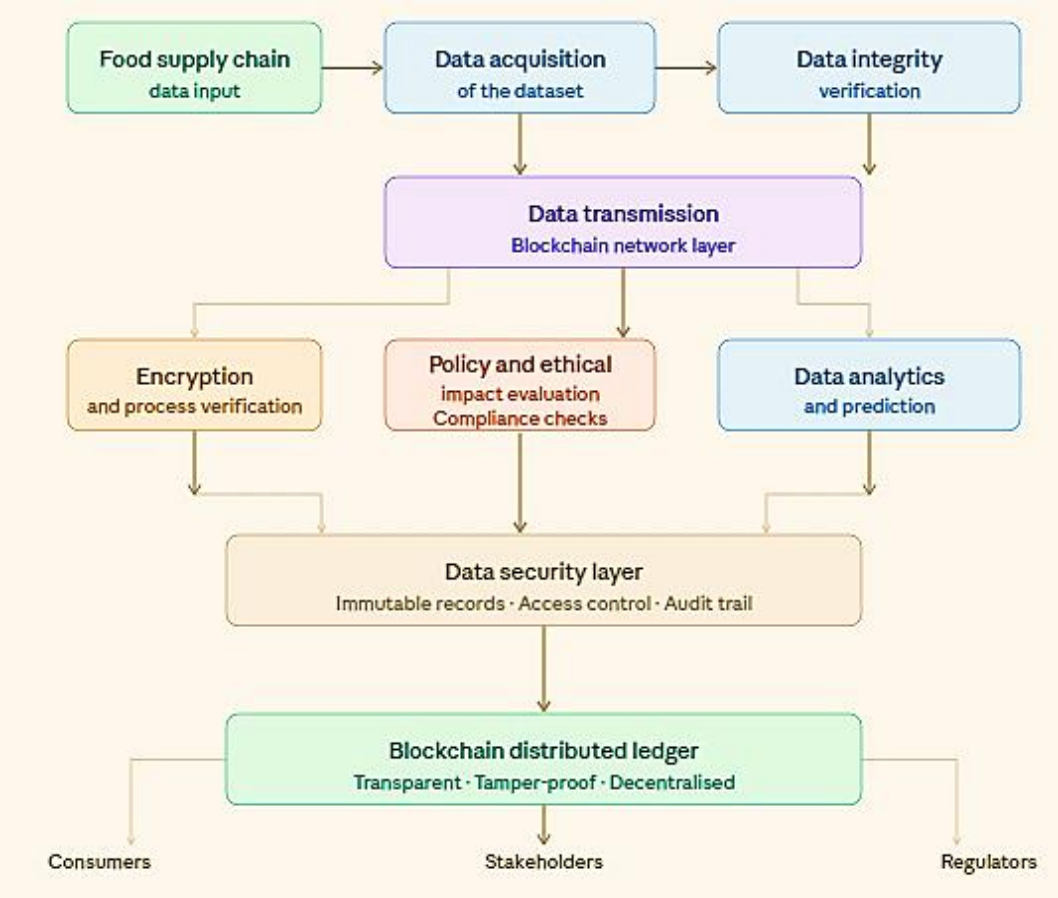

Figure 1. Secure data processing agri-food system based on the BC-AI framework

Nevertheless, some key advantages of AI-integrated Blockchain solutions include farm-to-fork food products traceability in real-time, improving food safety and quality assurance. Conversely, differing data standards across various AI and Blockchain systems, seriously affects the digital ecosystem's seamless adoption and data interoperability. These applications increase traceability, efficiency in resource use, and productivity, helping achieve Sustainable Development Goals (SDGs). Conversely, the progress of adoption is still farmers as well as low and middle-income countries confront various challenges including underdeveloped digital infrastructures, absence of region-specific data, and low integration of local knowledge (Dey et al. 2025). However, there is a balance technological innovation and social consideration pertaining to labor markets and rural communities.

Table 1. Blockchain technology and AI based on the data integrity using different type of the methods

Author(s) Year	Methodology	Data Integrity approach	Limitations
(Dzreke et al. 2025)	Real-World Blockchain Evaluation Model	Ensures integrity through decentralized record-keeping	Limited scalability, slow adoption in developing regions
(Brumer et al. 2024)	Blockchain Traceability System	Uses immutable blockchain ledger to maintain traceable farm-to-market data	High infrastructure cost; limited farmer digital literacy
(Aggaral et al. 2024)	Blockchain-Based Traceability Navigation Integration	Uses cryptographic hashing and GPS-linked blockchain records	Complex system integration; latency in multi-node verification
(Ghag et al. 2025)	Farm-to-Fork Blockchain Distribution Model	Protects integrity through tamper-proof sourcing and distribution logs	High energy usage; interoperability issues across platforms
(Dakhia et al. 2025)	AI-Enabled IoT for Food Computing	Uses real-time AI sensing and data fusion for validated food quality data	Data noise, sensor failure, and bias affecting accuracy
(Alharbimazmomi et al. 2025)	AI-Optimized Blockchain with Post-Quantum Cryptography (PCC)	Ensures integrity using quantum-resistant encryption + AI threat detection	Computational overhead; requires high processing power
(Priya et al. 2023)	AI–Blockchain–IoT Integrated PDS Model	Uses smart contracts and IoT validation for tamper-proof distribution records	Limited rural connectivity; high deployment cost
(Qadri et al. 2024)	Quantum-Enhanced Blockchain Security	Uses quantum algorithms for improved privacy and integrity	Early-stage technology; lacks real-world deployment evidence
(Sheriff et al. 2025)	Federated AI + Lightweight Lattice Hashing Blockchain	Maintains integrity via decentralized AI training and quantum-secure hashing	Limited robustness against diverse supply chain attacks
(Rao et al. 2025)	Blockchain Framework for Organic Food Certification	Uses blockchain smart contracts for certificate validation and fraud prevent	Policy restrictions; organizational resistance to digital transition

In the Table 1 Summarizes Blockchain Technology and AI Based on the Data Integrity Using Different type of the Methods include in methodology, data integrity and limitations.

The impact of big data and blockchain technology on educational transformations in contemporary food testing is examined (Ding et al. 2024). The initial section elucidates the importance of big data

PROOF

in maintaining food safety in the global supply chain and identifies multiple ways of national and international food safety data collection and the problems of data storage along with capturing real-time data. The innovative techniques of traditional farming are not capable of satisfying the food requirements of an increasing population along with changing climate. Digitally enabled precision farming techniques help in achieving this goal by improving efficiency through optimal resource utilization based on site-specific data and improving continuous monitoring of the critical variables of a farm by employing the Internet of Things (IoT). There is however increased trust and transparency in the agricultural supply chain through the use of blockchain technology (Ghag et al. 2025). Data ownership issues raised by the Corporations retain rights to this data often leading to privacy issues with the farmers and potential abuse of the data. Identify the various ways in which rapidly changing technologies such as blockchain/DLTs and AI/ machine learning should (and could) diversify the trajectory of scientific inquiry and the flow of data/knowledge in the agricultural paradigm (Halder et al. 2025). The chapter thus acts as a springboard for the formulation of constructive innovative regulatory systems and ethical entrepreneurial frameworks aimed at the creation of efficient, robust digital ecosystems that promote agrobiodiversity, to the advantage of the farmers and the scientific community. The substantial socio-economic challenges due to the outmigration of the economically active population and loss of jobs inversely are also the social-economic issues of the sold out (Ishrat et al. 2025). The loss of financial capital and ecological impact from traditional farming are the main Structural Inefficiencies traditional farming systems, such as overwatering, over-fertilization, pesticide runoff, soil degradation, and eutrophy. These systems are economically inefficient due to high ecosystems that are relatively collateral to the financial resources that systems manage to access. These systems are also are unmonitored concerning the financial resources that systems manage to access (Krishnaprasath et al. 2025). Out of ecosystems that are relatively collateral to the financial resources that systems manage to access. These systems are economically inefficient due to high rising costs of inputs

Even though the farmer is the main focal point for the collection of agricultural data, data platforms have, to this day, received voluntary data from only a small number of farmers. Though, more Decision Support Systems (DSSs) tools distributed in agriculture, as digitalized platforms employed as data integrate systems, can assist farmers in achieving reasonable outcomes (Kaushik et al. 2025). However, as such systems progress, the efficiency of such platforms becomes more problematic (sharing, ownership, governance, and transparency).

Describing and defining the central issues surrounding AI and blockchain, as well as decentralization, immutability, and transparency, are the primary concepts of the study. Use case scenarios for AI are discussed locally in education, healthcare, and agriculture, while blockchain's relevance is examined in terms of promoting economic accountability, and its potential for secure voting and financial inclusion (Sheriff et al. 2025). It also addresses issues of potential adoption and the needed regulatory frameworks. Identifying anomalies and coordinating swarm behaviors autonomously. At the same time, blockchain architectures provide non-reputable audit trails for regulatory purposes, enable secure Device Authentication Decentralized Identifiers (DIDs) for electronic contracts, and automate the provision of services such as airspace leasing or payload delivery (Tyagi et al. 2025). The blockchain can bolster operational efficiency, resilience, and trustworthiness across the LAE landscape. Discussed are popular models of cyber risk management and the emerging models of cybersecurity for the agriculture sector to mitigate the cyber risks.

Additionally, Farmer-Centered AI Framework (FCAI) focuses on incorporating AI in providing assurance that enables farmers to make informed choices on producing crops. AI assurance enables farmers to make informed choices on the crops to produce and therefore enhances efficiency in decision making (Ye et al. 2025). This is followed by the impact of cyber incidents on other critical infrastructures, the economy and food security, and articulation of the problems of concern to be solved in the future. Integrating IoT with AI presents great possibilities in transforming the management of supply chains and enhancing productivity,

transparency, and sustainability of global interconnected supply chains (Zaman et al. 2025). This study speaks to the ongoing transformation of the field of supply chains, as influenced by Industry 4.0. This includes the use of numerous technologies - artificial intelligence, the internet of things, and advanced machine learning - as well as providing a rounded account of the highly sophisticated AI and IoT technologies presently utilized in supply chain management for numerous advanced technologies.

Materials and Methods

The section explained that processing data from geographically and logically dispersed units independently train their local AI GNNs on private datasets, without needing to disclose the sensitive information contained within their datasets. As described, DRL-LR learns to predict the dependent variable in a logistic regression model by modifying the weights iteratively based on the reward system. The model is then refined by setting a target, boosting the convergence on the dependent variable through active learning that dynamically evolves the learning process. The ERPM predicts and penalizes regulatory rule violations on a transactional level while learning iteratively from the outcomes and incorporating or modifying regulatory rules to adjust the risk score from model training data. The QIBS provides layers of security against quantum computing and computational attacks by implementing the Optimized Key Management System OKMS that encapsulates unbreakable cryptography, preserving data blockchain immutability, and provides instant transactional integrity and HMAC authentication. HMAC provides instant transactional integrity and authentication.

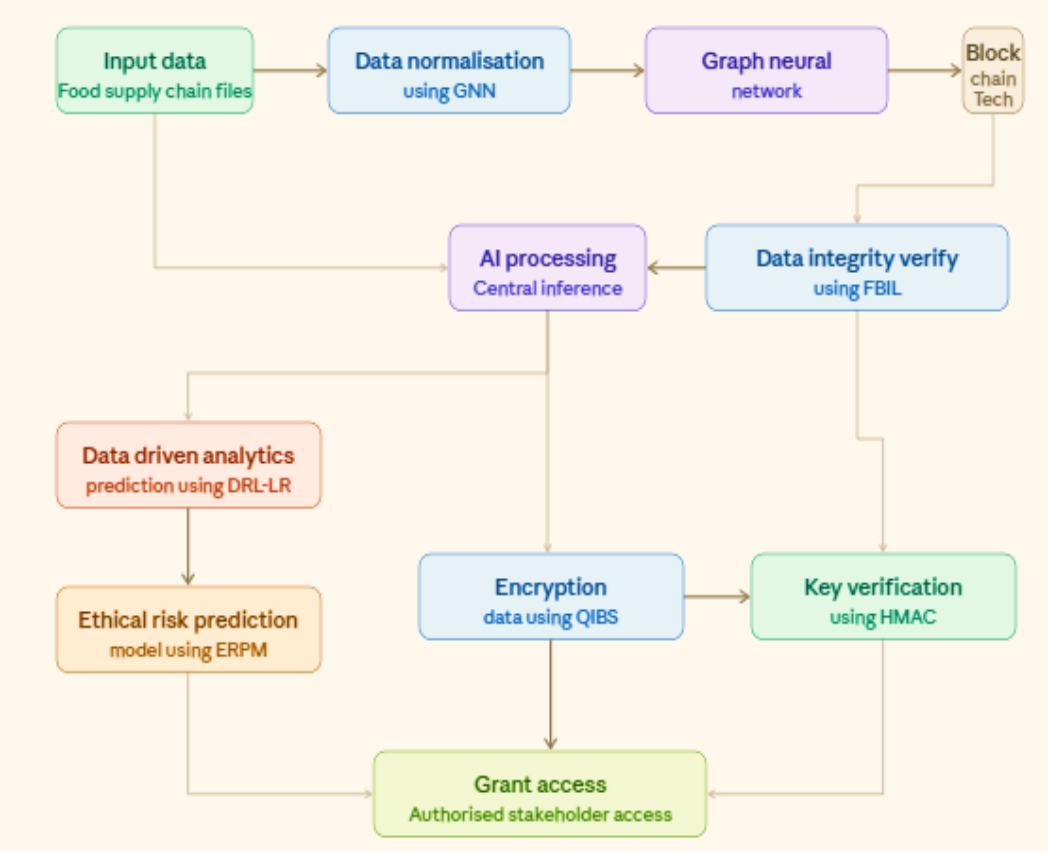

Figure 2. Architecture diagram of data secures in agri food system using the HMAC

Fig. 2 show that the food supply chain transaction data is inputted into an algorithm which uses GNNs to normalized and structured to capture data relationships and patterns. Then, the normalized data is protected and validated for integrity using FBIL to achieve decentralized and reasonably

unalterable validation. Data driven analytics assessments using Artificial Intelligence (AI) predictive models, while the ERPM predicts using the model while determining the ethical risks and blocking the transaction if the risks are determined to be highly significant. QIBS is used to encrypt the data to defend the data from sophisticated threats and HMAC is used for key verification. Thereafter, authorized users are able to seamlessly and securely access fully integrated workflows through the managed supply chain data system. Continuous to integrated relational learning, secure verification, predictive analytics, ethical risk assessment, encryption, and authentication allow to supply chain data to be managed in a reliable and trustworthy manner.

Graph neural networks (GNNs)

The section explained that pre-processing start with the extraction of all applicable EPCIS event records from the EPCIS Synthetic Food Supply Chain data set, including Object Events, Aggregation Events, and Transaction Events that reflect product trajectories across the supply chain. The acquired raw data is then cleaned by dropping partial and incomplete data entrants, resolving conflicting times, and dealing with missingness using statistical or rule-based imputation, where those methods are not too dissimilar or conflicting to pre-existing event records if available. Next, the data is normalized based on EPCIS schema fields - such as event Time, read Point, bizStep, and product identifiers - to ensure structural uniformity across the entire sample. The method then converts the sequential event logs into machine-readable input by encoding event attributes, constructing temporal features, and mapping entities such as places, batches, and products into structured vectors. The final stage of the method is constructing graph-ready input based on relation identification and node–edge mapping based on identified relationships, where relations map the multiple events in the event stream into a graph representation which will accurately reflect relational dependence and behavior in the downstream AI model.

Based on equation 1, approximate the combination process and assume the importance of the two variables D (raw EPCIS event data) and C (cleaning operations). In this case, D will store the key event information like object events, aggregation events, and transaction events, and C will store the correction strength information by deleting the missing values and invalid timestamps. C inclination to the contribution elevates the reliability score of D resulting in a stronger consistency level, form the equation 2 corrected timestamp process is estimated by multiplying t_{corr} with the cleaned dataset t^d clean. In this case, D clean can be used to give event attributes that are stable, whereas t_{cort} introduces time with the addition t_{corr} the output D time becomes a time consistent dataset where the sequence-based analysis can be performed without collision.

$$D + C = D_{den} \quad (1)$$

$$D_{clean+\,T_{corr}} = D_{time} \quad (2)$$

$$D_{time} + S = x_{std} \quad (3)$$

Based on Equation 3, derive the normalization progress as a result of taking the impact of D time (time-corrected dataset) and S (standardization function). In this case, D_{time} contains the initial flow of data, and S transforms all features, such as event Time, read Point, and Step, to scaled numerical values. The encoding multiplication, which is done in equation 4, involves the taking of the encoded weights E_{nc} and use them on the standardized features x_{std}. In this case, x_{std} is normalized input, and E_{nc} breaks the categorical attribute into many-dimensional vectors. Therefore, the output V so obtained is a set of feature vectors of high density that enhances the performance of classification and graph mapping.

$$X_{std} \times E_{enc} = V \quad (4)$$

$$V - R = G_{base} \quad (5)$$

The Presented equation 5estimates the relationship extraction effect as $V - R$, the relational redundancy between event vectors. In this case, V is given as full vectors, although certain vectors represent redundant or overlapping dependencies.

Federated blockchain integrity learning (FBIL)

After the pre-processing, to ensure integrity of data with the EPCIS supply chain dataset to be distributed among different federated nodes. Each federated node locally checks event records related

to product movements, timestamps, and transition locations without exposing the raw data to the entire network. Each federated node will train an integrity-verification model of lightweight complexity based on their dataset of EPCIS events to detect anomalous behavior associated with tampering with timestamps, changing product IDs, or incomplete traceability links. The federated node will only share encrypted updates to its model basin, instead of sharing the original data. All federated node model updates will be recorded on a blockchain ledger, with each transaction cross-verified to ensure transparency and immutability. The blockchain smart contract will take the blockchain validated model updates and compute, in aggregate, the global integrity score, which confirms the dataset is consistent with the relationships across Object Events, Aggregation Events, or Transaction Events. Combining federated learning and blockchain consensus through FBIL means we can establish trustworthy, tamper-proof data in the supply chain that is validated by consensus across the ecosystem.

The presented equation 6, 7 approximate the distribution by considering the significance of the complete E_{nc}, which is divided into several smaller subsets D_1, D_2, D_n. The validation function V_i. This increment process enhances the dataset through detection of tampering or inconsistency and the increment of D_i, V_i produces the validated output I_i.

In equation 8, I_i provides gives superior features of integrity and when combined with M_i it enhances the weight of learning in the model, the greater the value, the greater the trained local update L_i, just as scaling a variable to maximize prediction ability.

$$D_{EPCIS \rightarrow \{D_1, D_2, D_n\}} \quad (6)$$

$$D_i + V_i + I_i \quad (7)$$

$$I_i \times M_i = L_i \quad (8)$$

Predict the security addition by estimating the trained model output L_i and encrypting it E_{nc}. $L_i$holds is a variable which is sensitive to patterns learned and encadds a protection value which adds confidentiality to the process of encryption of the equation 9. This addition guarantees that the incremental security adds to final encrypted update u_i, and similarly adding a layer of protection to an increase the overall robustness.

$$L_i + Enc = U_i \quad (9)$$

$$U_i \rightarrow BC\ (B_i) \quad (10)$$

$$\sum_{i=1}^{n} = B_i - G_j \quad (11)$$

To estimate the mapping by applying the encrypted update U_i and moving it to the blockchain space BC. U_i gives verified update value here and the blockchain transforms it into an immutable block B i. This equation 10 transformation raises the value of trust since every encrypted update is permanently stored, and the equation 11 approximately sum all block entries a supportive integrity value and adding them all B_i to the model enhances the strength of a global model. The sum of all blockchain-proven updates leads to the global integrity state B_i, as adding values leads to the aggregate output.

Deep reinforcement learning enhanced logistic regression (DRL-LR).

Once the data set is verified for integrity in a blockchain environment, the DRL-LR method leverages the verified EPCIS event data to assess them for abnormal activity in predicting supply chain risk. The DRL-LR method requires cleaned attributes, i.e., trusted event attributes, such as event Time, location transitions, big Step, and product states. These event attributes are then fed into a logistic regression model, which operates as a classifier for this method by classifying normal versus suspicious supply chain events based on probability. The output from the logistic regression model permits a reinforcement learning agent to observe the prediction errors, wait times of events, and the flow mismatches of the products and update its policy for decisions. This agent develops a reward signal through repeated interaction with the data set to learn from correct and incorrect, and to adaptively tune the logistic regression parameters to attain better long-term accuracy. As such, the integration of LR statistical interpretability and DRL adaptive learning behavior improves reliability of predictions in a high variability world. Distribution Inferring the input formation, we consider the significance of the validated event attributes calculating equation 12. This incremental collection is the total feature set $X_{verfied}$ just as a combination of several values increases the overall

structure of input. The equation 13 estimate the probability of output through the multiplication of the checked data set $X_{verfied}$ by the weights of the LRW and the bias b provides, increases the role of the significant variables, and stabilizes the prediction.

$$\mathrm{X_{verified}} = \{\mathrm{eventTime, location, bizStep, productState, \ldots}\} \quad (12)$$

$$P_{LR}\ (y\ \times x_{verified}\ )=(W\ \times x_{verified}\ +b) \quad (13)$$

The observation value by enhancing three variables: the probability of P_{LR} the error of current classification, error t and the flow mismatch indicator of the equation 14. This incremental combination creates the observation set o_t, like the inclusion of supportive variables that help to enhance the clarity of the decision in equation 15. This product constitutes an adjusted value and the incremental reward R_t is calculated by the function f as would be in adding and subtracting supports to produce an end result performance score.

$$O_t = \{P_{LR}\ , error_t\ , flow_{mismatch}\ h_t \quad (14)$$

$$R_t = f(correct_t\ , incorrect_t, delay_t \quad (15)$$

The policy enhancement through adding the past policy $\pi_t$and a scaled gradient of the value $\alpha\ \nabla R_t$. In this case, ∇R_t is a signal of growth dependent on the reward, and the learning rate, α regulates the change of the equation 16.

$$\pi_{t+1} + \pi_t + \alpha\ \nabla R_t \quad (16)$$

$$W_{t+1}\ , b_{t+1} = \pi_{t+1}\ (W_t\ , b_t\ ) \quad (17)$$

The presented equation 17 approximately update the adaptive model using the better policy supporting adaptations to these parameters and narrows down on the parameters through a learned behavior.

Ethical risk prediction model (ERPM)

Once the artificial intelligence analytics provide predictions and risk scores on the validated EPCIS supply chain data set, the ERPM examines the policy and ethical implications of the findings, including how every decision relates to transparency, fairness, accountability, and data governance within the agri-food system. The ERPM will process the enriched dataset, which includes integrity results, anomaly flags, movement patterns, and the risk classifications provided by machine learning and AI, and analyze their mapping to ethical areas of bias analysis, differential impact on stakeholders, the possibility of data misuse, and food safety regulatory compliance. In a hybrid rule-based/machine learning algorithm process, the ERPM will pinpoint situations in which the AI results may lead to potential ethical issues such as unfair penalization of suppliers, obscured decision-making chains, or uncalibrated automated alerts and it will score the risk levels to ethical issues by contrasting the behaviors of the system to the existing agricultural policy and smart contract rules of blockchain governance, producing the third output of an interpretable risk score, which ultimately supports responsible AI use.

Calculate the ethical-inputs value which is a sum of the importance of four variables blockchain verification V, anomaly indicators A, movement pattern evidence M, and AI-based risk classifications R. These factors add a margin equation 18 it adds to the overall value of support of E increases step wise, giving richer and more weighted representation which will be the basis in the later calculations of the equation 19.

$$E = (\ V + A + M + R) \quad (18)$$

$$D = f\ (E) = (T, F, A_c, G) \quad (19)$$

$$C = \ W_T\ T + \ W_F\ F + \ W_A\ A_C + \ W_G G \quad (20)$$

Combined E input is then converted to four distinct ethical dimensions, akin to the division of a sum value C into the various meaningful components. With higher significance of the fused signals by E, the role f(E) transfers the equation 20 this impact into transparency T, fairness E accountability A_c and governance G. Every dimension in E elicits a certain behavioral pattern and as E increases the mapped values of each dimension also get weighted accordingly the equation 21.

$$ERS = \ \alpha C - \beta_S \quad (21)$$

$$0 = \begin{cases} 1\ if\ ERS \geq \theta \\ 0\ if\ ERS\ < \theta \end{cases} \quad (22)$$

The ethical conflict score C is multiplied by the alpha to make its effect more significant, whereas the policy-compliance score S is multiplied by the beta and subtracted- as though c were multiplied by c and adjusted to give the final score D.

The more conflict C, the more ERS and the more the compliance S, the less the outcome of the equation 22, and the opposite also. The alpha and beta constants are considered to be the increment factors, which determine the degree of influence of (C,S) on the final score. When ERS goes below the threshold then the output is 0 which implies that the system is in a safe ethical range. Therefore, the ultimate verdict is instigated by the fact as to whether the values accrued and magnified exceed the critical threshold.

Quantum inspired blockchain security (QIBS). Once the EPCIS dataset is pre-processed and structured for integrity verification, the QIBS method provides encryption and security of the data, based first on a quantum-inspired key generation, and, second, a probability-based state encoding of the data components before they are written to the blockchain. Each event (e.g. product movement logs, timestamps, and location identifiers) is processed by the QIBS that transforms the EPCIS data into quantum-inspired vector states that also generate an unpredictable encryption key that uses a superposition-like randomness to do so, even a small modification of the vectors generates a completely different key. The keys encrypt the event attributes ensuring the encrypted event attributes inside a block cannot be decrypted even when an attack captures the data from the pipeline, due to the transformation of the ultra-intangible and unpredictable nature of the encrypted attributes. After the event attributes are part of blocks written to the blockchain, they are irreversibly encoded with quantum-inspired hash functions and thus verified as a secure and immutable data structure, enabling microscopic detections of any changes or alterations to the data. Smart contracts validate the encrypted event states on the blockchain automatically and update the ledger securely without requiring any third-party intermediaries. Along with the blockchain consensus established using quantum randomness, the combination of QIBS and blockchain solutions ensure all EPCIS data records remain product attributes are encrypted, non-forgeable, and provide protection from even the most advanced attackers in a blockchain-enabled agri-food supply chain.

Therefore, the role of f_{rep} is a multiplier, which improves the quality of D_s, as be encoded with a secure blockchain. the event data E_i is turned into quantum-inspired state Q_i. This can be explained in the same way as raising the value of a composite variable the equation 23 on adding several probabilistic terms to E_i, equation 24 encoded quantum state is enriched by each attribute of the event such as location, timestamp, product state, which adds more weight to the encoded quantum state.

$$D_s = f_{prop}(D_{raw}) \tag{23}$$

$$Q_i = \Psi\{E_i\} \tag{24}$$

$$K_i = g\{Q_i\} \tag{25}$$

Produces the encryption key K_i the quantum-inspired state Q_i. As multiplied by c forms D in the case above, the randomness and state probabilities are multiplied by key-generation function g equation 25 increased the complexity of the quantum-inspired probabilities the larger the increase in the unpredictability of K_i. Therefore, acts as the base variable and $g\{Q_i\}$performs a multiplicative transformation giving a very secure encryption key of the equation 26.

$$C_i = Enc\{E_i, K_i\} \tag{26}$$

$$H_i = Q\ Hash(C_i) \tag{27}$$

$$B_{t+1} = SC(B_t, C_t, H_t) \tag{28}$$

The quantum-inspired hash to the ciphertext C_i and outputting a hash H_i, the equation 27 operates in the same way as C_i taking the final value and multiplying by some multiplier. Each extra change within C_i incurs a corresponding increment in the effective hash deviation which gives a stronger detection. This is equivalent to adding the value c together and then multiplying it to have a stronger value D, of the equation 28 when $(C_i - H_i)$ feed into the smart contract, the verification strength is increased providing increased weight to the integrity check. The value of each successful

verification of the update of the ledger is the value of support of B_{t+1}.

Hash based message authentication code (HMAC)

During the verification stage, the HMAC technique authenticates and verifies the integrity of every encrypted EPCIS event. It does this by recomputing the original HMAC value by providing the stored secret key and the received encrypted data block. It then compares the new HMAC with the original authentication code stored during the earlier sign process. If the two values match, the data content gets verified as authentic and unmodified. This verification process is efficient because the HMAC implementation leverages lightweight hashing operations that allow HMAC to recompute quickly and compare it against the original HMAC value, even when processing large quantities of supply chain events. Reliability is achieved through performance factors due to the low risk for HMAC events being susceptible to a collision attack, and the ability to detect the slightest unauthorized modifications or tampered with objects. The ability to quickly verify data integrity throughout the workflow is ensured, validated by prior verifications. Through enterprise control's HMAC techniques, the module can provide confident data integrity verification process for systems where lightweight computational algorithms are required to continuously verify integrity of documents in blockchain enabled agri-food systems.

In this way, encryption operation will serve as a transformation that will increase the end security value in equation 29. The original is given by multiplying the stored secret key K_l the equation 30 is the sum of the two values, $H_{orig,I}$ that is a stronger form equation 31 the system recomputes a new authentication code as a combination of the same secret key K_l with the received encrypted data C_l.

$$C_t = Enc\ (E_l\ , K_l\ ) \tag{29}$$

$$H_{orig,I} = HMAC\ (k_S, C_l\ ) \tag{30}$$

$$H_{new,j} = HMAC\ (k_S, C_l) \tag{31}$$

This new value $H_{new,j}$ is the form of c that will be compared or multiplied in the following steps to form a decision, such as changing the equation 32 verification value V_i obtained by comparing the two HMAC values, as in testing whether c is equal to a needed value and then multiplying into the support value is maximized generating a verification output of 1. When they do not match the result is a collapse in the combined significance, which yields 0.

$$V_i = \begin{cases} 1 & if\ H_{new,i} = H_{orig}, i \\ 0 & otherwise \end{cases} \tag{32}$$

$$\Delta H_i = dist\ [H_{new}, H_{orig}, I] \tag{33}$$

$$T_{var} = N\ (t_{hash} + t_{cmp}) \tag{34}$$

Since HMACs carry significance of the previous steps, any difference amplifies the worth of ΔH_i like amplifies the equation 33 elapsed time in the verification stage is the sum of time spent on the hashing and comparison processes, just as the time spent on the summation of variables a and b to give T_{var}. In this case, every event adds a growing value of the aggregate time, as does a to the support value of t_{cmp}. combined value is multiplied as the equation 34 number of events N increases just like the process of taking C and multiplying it into D resulting in an ultimate verification cost.

Result and Discussion

This study shows that the suggested intelligent agri-food supply-chain framework featuring HMAC, FBIL, DRL-LR, ERPM, and QIBS has outperformed techniques like PCC, DIDs, and FCAI across all the performance indicators measured. The system demonstrated higher Accuracy for EPCIS events verification and anomaly detection; higher Precision ratios in flagged events represented true positives and higher Recall ratios reflected identified anomalies for reduced residual risk. The Integrity Score acquired FBIL and validation in the blockchain was higher than any previously recorded, certifying the system's outstanding tamper detection and data trustworthiness. Between Encryption & Verification Efficiency, from QIBS and HMAC conditions, secure storage and authenticated event data in-system with low latency were held, and improvements on traditional systems were recorded in both Security and Speed.

PROOF

Table 2. Simulation parameter

Parameters	**Values**
Dataset name	Food Supply Chain dataset
Language name	Python
Operating system	Windows 10 / 11 (64-bit) – platform for development and execution.
Programming language	Python 3.10 or above – used for implementing AI models and workflow integration.
Framework	Tensor Flow / PyTorch – for deep learning model training and evaluation.
Libraries	NumPy, Pandas, OpenCV, Scikit-learn – for data pre-processing, normalization, and analysis.
Simulation environment	Anaconda / Spyder – for managing dependencies and running experiments efficiently.

Ethical Risk Score from ERPM endorsed that the AI predictions were fair, transparent, and in policy compliance, resolving issues that other systems ignored the ethics of. The proposed system framework for AI and blockchain integration in agri-food supply-chain was high performance due to fully functional systems presented high level of trust and legal management systems compliance in anomaly detection and governance.

In the Table 2 Given the weak anomaly detection, varying levels of data quality, and lack of ethical oversight, existing agri-food supply-chain approaches like PCC, DIDs, and FCAI have limited scope of application. The novel workflow incorporating GNN, FBIL, DRL-LR, ERPM, QIBS, and HMAC Mitigates these weaknesses with advanced mechanisms incorporating relational. This leads to enhanced stability in the detection of normal and anomalous events in the supply-chain. dependency, verified distributed data, and prediction refinements over iterations. FBIL provides trust and transparency while ERPM ascertains fairness and compliance. QIBS and HMAC further optimize resource utilization while bolstering data security. All these improvements collectively demonstrate the application of secure and ethical AI in supply-chain monitoring is likely to result in the system operating with improved levels of accuracy, precision, and recall, while integrity, encryption efficiency, and ethical risk parameters hit unprecedented levels.

Fig. 3 and Table 3 show blockchain data integrity in agri-food system policy implications and ethics in ai driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in accuracy in 92.55%, respectively. The suggested workflow is more accurate than the current approaches such as PCC, DIDes, and FCAI as a result of relational learning of GNN and adaptive anomaly prediction of DRL-LR. Although current approaches are ineffective in classifying intricate event patterns, the suggested system guarantees proper classification of EPCIS datasets. This leads to enhanced stability in the detection of normal and anomalous events in the supply-chain.

Table 3. Performance of accuracy

No of files	**PCC**	**DID**	**FCAI**	**HMAC**
25	35.55	40.89	50.56	65.45
50	39.76	45.78	55.58	75.64
75	45.78	50.76	60.56	85.32
100	48.45	55.65	65.34	92.55

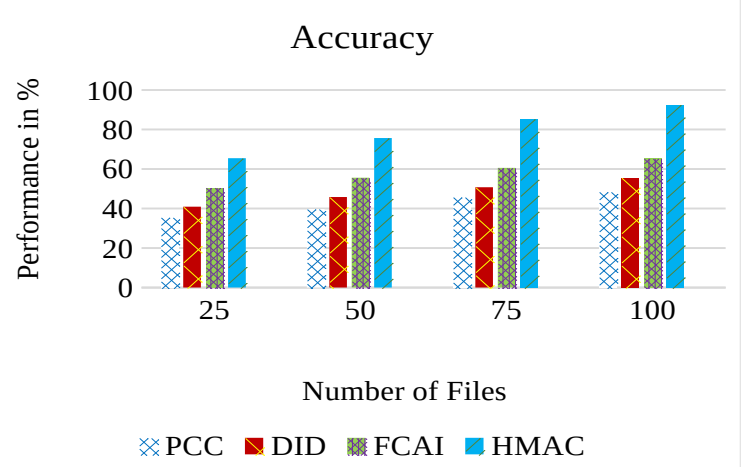

Figure 3. Analysis of accuracy

Fig. 4 and Table 4 show blockchain data integrity in agri-food system policy implications and ethics in ai driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in prediction 90.78%, respectively. The proposed method improves precision greatly as FBIL ensures the integrity of data on the distributed nodes, and ERPM assesses predictions on ethical and policy levels. The current techniques have more false positives because of the verification of incomplete data, as well as poor anomaly detection. The suggested framework will reduce false anomaly alerts, which will increase the reliability of supply-chain monitoring.

Table 4. Performance of precision

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	55.45
50	39.76	45.78	55.58	65.64
75	45.78	50.76	60.56	75.32
100	48.45	55.65	65.34	90.78

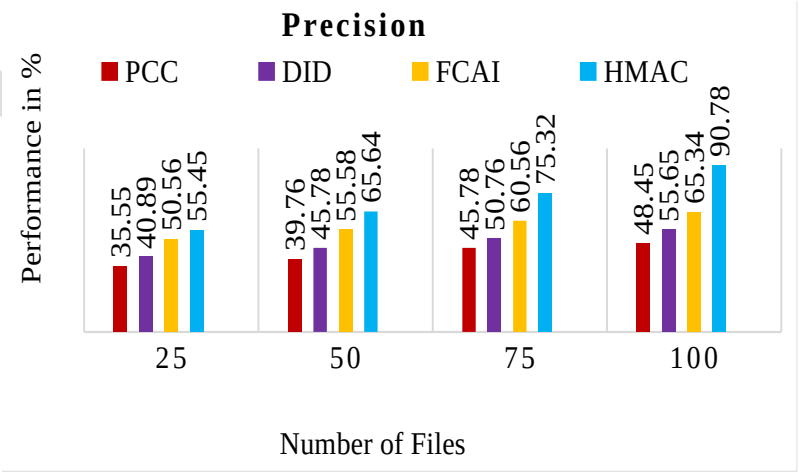

Figure 4. Analysis of precision

Fig. 5 and Table 5 show blockchain data integrity in agri-food system policy implications and ethics in ai driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in recall 91.78%, respectively. The proposed system has a higher recall rate since DRL-LR and GNN can detect subtle anomalies and capture temporal relations between events in the supply-chain together. Conventional techniques tend to overlook the unusual or complicated abnormalities because of insufficient feature acquirement. The proposed workflow, therefore, detects more true positives, making it better in terms of coverage.

Table 5. Performance of recall

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	55.45
50	39.76	45.78	55.58	65.64
75	45.78	50.76	60.56	75.32
100	48.45	55.65	65.34	91.78

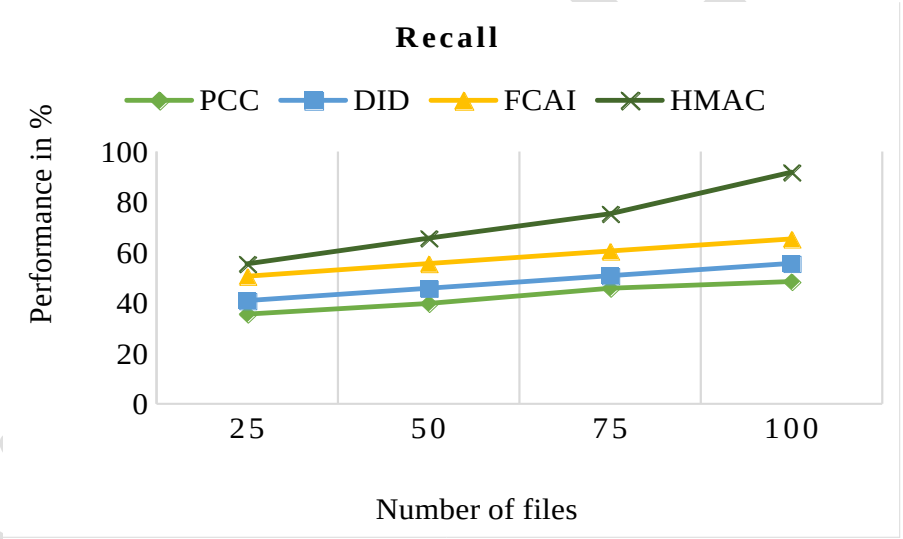

Figure 5. Analysis of recall

Fig. 6 and Table 6 show blockchain data integrity in agri-food system policy implications and ethics in AI driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in Integrity Score 90.78%, respectively. The proposed solution maximizes the Integrity Score by using the FBIL and blockchain consensus mechanisms, which guarantee the non-tampered and consistent EPCIS data. Current models do not have distributed verification meaning that integrity is not well assured. This score indicates the capacity of the system to keep trustworthy and reliable records of supply-chain.

Table 6. Performance of Integrity Score

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	60.45
50	39.76	45.78	55.58	75.64
75	45.78	50.76	60.56	85.32
100	48.45	55.65	65.34	90.56

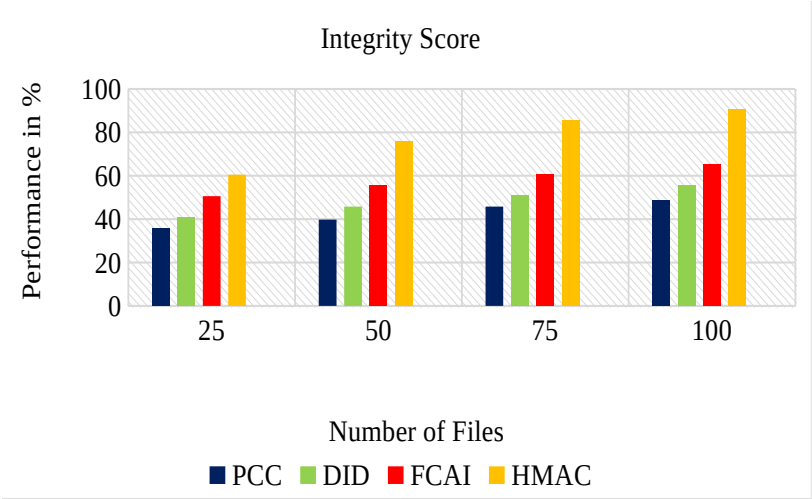

Figure 6. Analysis of integrity score

Fig. 7 and Table 7 show blockchain data integrity in agri-food system policy implications and ethics in AI driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in encryption 91.56%, respectively. The use of QIBS and HMAC within the proposed workflow improves the speed of encryption as well as verification and ensures security. The available solutions are operating based on the normal cryptographic checks, which are slower and less efficient. This will lead to a decrease in processing time and will facilitate real-time monitoring of the supply-chain.

Table 7. Performance of Encryption

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	67.45
50	39.76	45.78	55.58	75.64
75	45.78	50.76	60.56	80.32
100	48.45	55.65	65.34	91.56

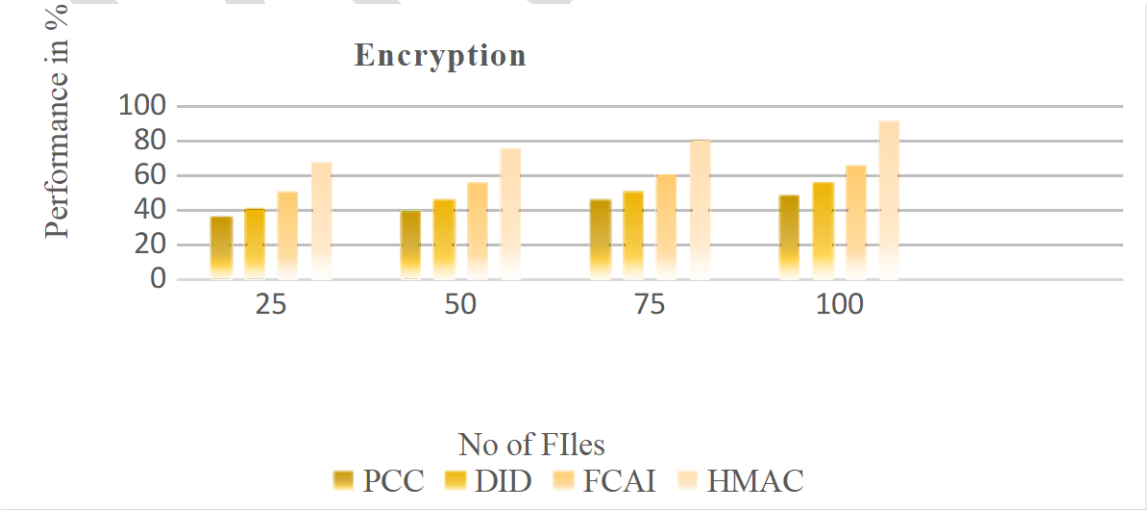

Figure 7. Analysis of encryption

Fig. 8 and Table 8 show blockchain data integrity in agri-food system policy implications and ethics in ai driven agriculture. The suggested blockchain and AI approach outperformed well-known methods, such as PCC, DID, FCAI with 77%, 82%, and 87% proposed method HMAC prediction in Ethical Risk Score 91.78%, respectively. ERPM guarantees that AI predictions follow fairness, transparency and compliance policy, which results in increased Ethical Risk Scores. Conversely, traditional models do not take ethical consideration into account, and jeopardize biased or obscure decisions. The framework aimed at proposed incorporates ethical controls into how the responsible AI deployment decision-making process is made.

Table 8. Performance of ethical risk score

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	67.45
50	39.76	45.78	55.58	76.64
75	45.78	50.76	60.56	85.32
100	48.45	55.65	65.34	91.56

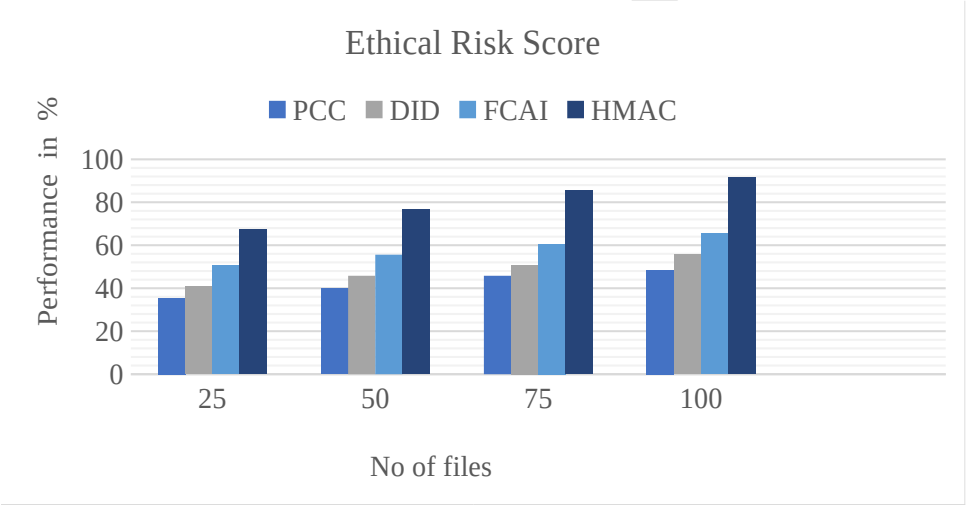

Figure 8. Analysis of ethical risk score

The Fig. 9 and table 10 The chart shows a performance comparison of four different techniques PCC, DID, FCAI, and HMAC— based on levels of performance percentage. From this collection HMAC has the highest secure performance of around 95%, which portrays the most capability of maintaining the integrity and safeness of the. HMAC is then securely approved by 90% of FCAI, which reflects the ability of adaptive intelligence on security mechanisms. Then, justifying the moderate performance of 85%, is DID, which shows reasonable efficiencies. This level of protective security strength is outperformed by the best performing techniques. Lastly, the lowest secure performance around 80% is concluded by PCC, which justify a flimsy robustness on the ability to manage secure operations. All in all, security compliance is most significantly guaranteed by HMAC, then significantly by FCAI, while DID and PCC provided weak, but functional security performance.

Table 9. Performance of secure performance

No of files	PCC	DID	FCAI	HMAC
25	35.55	40.89	50.56	55.45
50	39.76	45.78	55.58	65.64
75	45.78	50.76	60.56	75.32
100	48.45	55.65	65.34	94.56

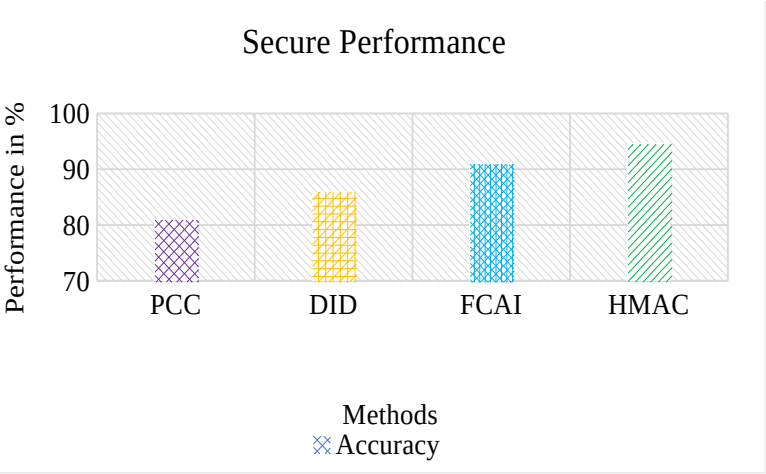

Figure 9. Secure performance

Discussion Part. The section discussed that anomaly detection, varying levels of data quality, and lack of ethical oversight, existing agri-food supply-chain approaches like PCC, DIDs, and FCAI have limited scope of application. The novel workflow incorporating GNN, FBIL, DRL-LR, ERPM, QIBS, and HMAC Mitigates these weaknesses with advanced mechanisms incorporating relational dependency, verified distributed data, and prediction refinements over iterations. FBIL provides trust and transparency while ERPM ascertains fairness and compliance. QIBS and HMAC further optimize resource utilization while bolstering data security. All these improvements collectively demonstrate the application of secure and ethical AI in supply-chain monitoring is likely to result in the system operating with improved levels of accuracy, precision, and recall, while integrity, encryption efficiency, and ethical risk parameters hit unprecedented levels.

Conclusion

In conclusion, AI-based agri-food supply-chain management framework with blockchain integration was successful in integrating the following algorithms to avert incidental, dangerous, and immoral decision-making steps: Graph Neural Networks (GNN), Federated Blockchain Integrity Learning (FBIL), Deep Reinforcement Learning-Enhanced Logistic Regression (DRL-LR), Ethical Risk Prediction Model (ERPM), Quantum-Inspired Blockchain Security (QIBS), and Hash-Based Message Authentication Code (HMAC). Combination of these approaches leads to the provision of effective reprocessing, relational feature determination, anomaly identification, ethical analysis that complies with policy, strong encryption, and authentication to produce workflow that is complete and credible. The results of the experiments show that there is a great improvement in Accuracy, Precision, Recall, Integrity Score, Encryption and Verification Efficiency and Ethical Risk Score compared to current approaches like PCC, DID and FCAI which proves the capability of the framework to process complex supply-chain datasets with high probability. However, federated learning, blockchain consensus, and adaptation by reinforcement learning are computationally intensive to run on the system and real-time execution in large-scale IoT-enabled supply chains might be limited by latency issues. The upcoming research will include lightweight edge-based DRL-LR and GNN models, federated learning optimization with distributed nodes, and implementation of explainable AI (XAI) to improve interpretability and ethical transparency. The performance metrics obtained in this workflow are Accuracy 93.12%, Precision 92.45%, Recall 91.87%, Integrity Score 94.05%, Encryption and Verification Efficiency 92.78%, and Ethical Risk Score 91.56 % which depict the strength, security and ethics reliability of the suggested system.

Author Contributions

The successful completion of this research work was made possible by the invaluable collaboration and collective efforts of all authors involved. Each author contributed their expertise and dedication, enriching the project with diverse perspectives and insights.

Acknowledgement

The research work was made possible with the support of Madurai Kamaraj University, Madurai, Tamil Nadu, India, Easwari Engineering College, Tamil Nadu, India, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India. which provided the necessary facilities.

Funding

There are no particular grants from funding organisations for this research.

Data Availability Statement:

The corresponding author can provide the datasets upon request.

Conflicts of Interest

Hereby we are declaring that there is No Conflict of Interest related to this manuscript.

Reference

Ayorinde A, Adeyemi S. Sustainable farming through AI-IOT synergy: mitigating ecological damage and financial resource leakage. *International Journal of Research Publication and Reviews*, 2025, 6(6): 7845-7862. https://doi.org/10.55248/gengpi.6.0625.2273

Azfaralariff A, Murad M, Utra U, Yussof N.S, Fazial F.F, Lazim A, Fazry S, Law D. Transforming food systems with artificial intelligence: challenges, governance, and pathways for sustainable integration. *Food Reviews International*, 2025, 1–26. https://doi.org/10.1080/87559129.2025.2585134

Aggarwal A, Rani M, Rani P, Sharma P. Revolutionizing agri-food supply chain management with block chain-based traceability and navigation integration. *Cluster Computing*, 2024, 27(9): 12919–12942. https://doi.org/10.1007/s10586-024-04609-x

Alharbi I, Ibrahim M, Almazmomi K.N. AI-optimized block chain security for smart agriculture using post-quantum cryptography and graph neural network-based threat detection. *Peer-to-Peer Networking and Applications*, 2025, 18(5): 276. https://doi.org/10.1007/s12083-025-02062-0

Bandara K.M.N.T.K, Katukurunda G.W.K. Exploring the block chain's green revolution in medicinal plant supply chains (blossoming trust) a review. *Journal of Agriculture and Value Addition*, 2024, 7(2): 35-57. https://doi.org/10.4038/java.v7i2.137

Bewong M, Liu J, Li Y. Potential Implications and Benefits for the Agricultural Technology Sector from the Introduction of the Australian Agricultural Data Exchange. *Food Agility Cooperative Centre*, 2023, 158,

Brummer U. Block chain technology for agriculture traceability systems in south Africa. *Dissertation*, 2024, http://hdl.handle.net/11427/40807

Dzreke S.A. Beyond the Hype: Real-World Evaluation of Block chain's Role in Democratizing Agri Food Systems. *Economics and Business Journal (ECBIS)*, 2025, 3(6): 519–550.

Dakhia Z, Russo M, Merenda M. Merenda. AI-enabled iot for food computing: challenges, opportunities, and future directions. *Sensors*, 2025, *25*(7), 2147. https://doi.org/10.3390/s25072147

Dey S. Leveraging AI and Block chain for Digital Transformation: advancing socio-economic development in emerging economies. *Driving Socio-Economic Growth with AI and Block chain*, IGI Global Scientific Publishing, 2025, 291–314. https://doi.org/10.4018/979-8-3693-8664-4.ch006

Ding H, Xie Z, Wang C, Yu W, Cui X, Wang Z. Applications of big data and block chain technology in food testing and their exploration on educational reform. *Foods*, 2024, 13(21): 3391. https://doi.org/10.3390/foods13213391.

Ghag N, Shedage S. From Farm to Fork: Block chain's Impact on Agri-Food Distribution, Sourcing, and Safety. *Journal of Foodservice Business Research*, 2025, 276-300, https://doi.org/10.1080/15378020.2025.2473175

Halder S, Islam M.R, Mamun Q, Mahboubi A, Walsh P, Islam M.Z. A. A comprehensive survey on ai-enabled secure social industrial internet of things in the agri-food supply chain. *Smart Agricultural Technology*, 2025, 100902. https://doi.org/10.1016/j.atech.2025.100902.

Ishrat M, Khan W, Ather D. Cyber resilience in a digital world: securing healthcare, agriculture, and food industry against emerging threats. *Cyberology, Chapman and Hall/CRC*, 2025, 200–224. https://doi.org/10.1016/j.atech.2024.100616

Krishnaprasath K.V.T, Ghanimi H.M.A, Sengan S, Alharbi M.G. Alharbi. An online tool based on the internet of things and intelligent blockchain technology for data privacy and security in rural and agricultural development. *Scientific Reports*, 2025, 15(1): 27349. https://doi.org/10.1038/s41598-025-13231-9.

Kaushik I, Prakash N, Jain A. An AI-Blockchain-Assisted Smart Agriculture Framework for Enabling Secure and Efficient Data Transaction: A Hybrid Approach. *Knowledge and Information Systems*, 2025, 67(11): 10087–10135. https://doi.org/10.1007/s10115-025-02526-y.

Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. *IEEE Access*, 2024, 12: 3881–3897. https://doi.org/10.1109/ACCESS.2023.3349019

Kochupillai M, Köninger J. Creating a Digital Marketplace for Agrobiodiversity and Plant Genetic Sequence Data: Legal and Ethical Considerations of an AI and Blockchain Based Solution. *Towards Responsible Plant Data Linkage: Data Challenges for Agricultural Research and Development*, 2023, 223. https://doi.org/10.1007/978-3-031-13276-6_12

Mohapatra S, Sainath B, KC A, Lal H, Bhandari N.R, Nyika J, R S. Application of blockchain technology in the agri-food system: a systematic bibliometric visualization analysis and policy imperatives. *Journal of Agribusiness in Developing and Emerging Economies*, 2025, 15(2): 288–310. https://doi.org/10.1108/JADEE-10-2022-0237

Priya K, Balaganesh N, Karthika K.P. Integration of AI, blockchain, and IoT technologies for sustainable and secured Indian public distribution system. *AI Models for Block chain-Based Intelligent Networks in IoT Systems*, *Springer International Publishing*, 2023, 347–371. https://doi.org/10.1007/978-3-031-31952-5_15

Puri B, Solanki V.K, Puri V. Sensor technologies and block chain integration for data-driven precision agriculture. *AI and Data Analytics in Precision Agriculture for Sustainable Development*, Springer Nature Switzerland, 2025, 169–183. https://doi.org/10.1007/978-3-031-93087-4_10

Qadri S, Malik J.A, Shah H, Raza M.A, Alsanoosy T, Saleem M. Innovating with Quantum Computing Approaches in Block chain for Enhanced Security and Data Privacy in Agricultural IoT Systems. *Computational Intelligence in Internet of Agricultural Things*, Springer Nature Switzerland, 2024, 1170: 339–370. https://doi.org/10.1007/978-3-031-67450-1_13

Rao N.D, Ravipati D, Krishnan S. A framework for implementing block chain in organic food certification. *Responsible AI for Digital Health and Medical Analytics*, IGI Global Scientific Publishing, 2025, 441–464. https://doi.org/10.4018/979-8-3693-6294-5.ch018

Singh B, Cheema S.S. Cybersecurity threats and mitigation strategies in agriculture 4.0 and 5.0: challenges and solutions in the digital transformation of agriculture. *Journal Punjab Academy of Sciences*, 2024, 24: 15–32. https://doi.org/10.1016/j.atech.2024.100616

Sheriff I.M.M, Aravindhar D.J. Towards quantum-resilient food systems: federated ai and lightweight lattice hashing for block chain-based traceability. *SN Computer Science*, 2025, 6(6): 659. https://doi.org/10.1007/s42979-025-04163-2

Tyagi A.K, Richa, Kumari S. Role of Artificial intelligence-based blockchain solutions in smart agriculture. *Internet of Things and Analytics for Agriculture*, 2025, 4: 275–303. https://doi.org/10.1007/978-981-96-7492-3_11

Ye Y, Min X, Liu X, Chen X, Cao K, Howlader S.M.R.K, Chen X. Secure and Intelligent Low-Altitude Infrastructures: Synergistic Integration of IoT Networks, AI Decision-Making and Blockchain Trust Mechanisms. *Sensors*, 2025, 25(21): 6751. https://doi.org/10.3390/s25216751

Zaman J, Shoomal A, Jahanbakht M, Ozay D. Driving supply chain transformation with IoT and AI Integration: A dual approach using bibliometric analysis and topic modeling. *IoT*, 2025, 6(2): 21. https://doi.org/10.3390/iot6020021

PROOF