AI and Blockchain in Critical Food Supply Infrastructure: Cybersecurity Threats and Solutions

1st Mukter Khan
Department: Cybersecurity
Washington University of Science and
Technology
Virginia, United States
mdmuktar143783@gmail.com

2nd Md Solaiman Ahmed
Department: Cybersecurity
Washington University of Science and
Technology
Virginia, United States
Imhsolaiman@gmail.com

3rd Ratul Bhattacharjee
Department: CSE
American International University
Bangladesh
Dhaka, Bangladesh
ratulrahulbhattacharjee@gmail.com

Abstract: The escalating digitization of food supply chains (FSCs) has exposed them to significant cybersecurity threats, endangering food safety, integrity, and operational efficiency. This study presents a robust framework integrating blockchain and artificial intelligence (AI) to counter these challenges. Blockchain technology, with its decentralized and immutable ledger, ensures transparent and tamper-proof traceability, while AI's capability for real-time data analysis enables anomaly detection, predictive maintenance, and fraud prevention. Edge computing complements this framework by enabling localized data processing, thereby reducing latency and enhancing cyber-resilience.

Methodologically, the study combines a systematic literature review with simulated experiments to evaluate the efficacy of the integrated framework. The results are compelling: the framework achieves 92% accuracy in anomaly detection, reduces food fraud incidents by 40%, and boosts operational efficiency by 25%. Additionally, the fusion of edge-AI with blockchain slashes data processing latency by 30% in comparison to traditional cloud-based systems. These improvements effectively mitigate data integrity attacks, insider threats, and network-based vulnerabilities while preserving end-to-end traceability.

The study's findings highlight the potential of AI and blockchain to revolutionize FSCs, making them more secure, transparent, and efficient. However, challenges such as scalability, cost-effectiveness, and regulatory compliance need further exploration. This research not only offers actionable insights for developing resilient food supply infrastructures but also outlines priorities for future research, including the creation of advanced insider threat detection models and the implementation of robust security protocols. Overall, the proposed framework represents a significant step toward securing FSCs in an increasingly digital world.

***Keywords**: Food Supply chain, Blockchain, Artificial Intelligence, Cyber-physical Security, Traceability, Food Fraud prevention, Edge-AI.*

1. INTRODUCTION

The global food supply chain (FSC) is an immensely important factor for maintaining public health, economic and national security. But the complexity and interdependence of today's FSCs and the increasing worldwide thirst for food also pose tremendous problems concerning efficiency, transparency, security and sustainability. Researchers automate food systems and digitalized through the use of technologies like artificial intelligence (AI), blockchain, and internet of things (IoT), so also has the incidence of cyber security threats and operational failures increased significantly [1], [2]. The newly emerging risks, such as cyber-physical attacks, data breaches and disruption of supply chain threaten the integrity and the resilience of the food business [3], [4].

Current research has made substantial progress in applying AI and blockchain individually to address specific issues within FSCs. Nevertheless, there is a notable gap in studies that systematically integrate these technologies, particularly in conjunction with edge computing, to holistically enhance cybersecurity and operational resilience. This study aims to fill this gap by proposing a unified framework that leverages the complementary strengths of AI, blockchain, and edge computing. While existing literature has touched on the individual applications of these technologies, our research demonstrates how their integration can lead to a more secure, efficient, and transparent FSC. The novelty of this approach lies in its comprehensive methodology, which not only improves traceability and fraud prevention but also addresses real-time operational challenges through edge computing.

1.1. Cybersecurity Threats and Vulnerabilities in Food Supply Chains

As digital technologies quickly infiltrated food production and processing to distribution, traditional food supplies chain management systems are now challenge with cyber threats [5]. Operational technologies (OT) including automated control systems, IoT devices, cloud-based systems are critical for operating food supply chains with high efficiency but come with a loophole for cybercriminals to exploit [6]. Cybersecurity threats such as cyber-physical attacks and Advanced Persistent Threats (APTs) are a grand challenge to the security and functionality of food systems [7], [8]. Cyber-attacks on industrial control systems (ICS) in food plants, for example, can create safety hazards, product contamination, and costs [9], [10]. The lack of real time visibility into operations, especially large-scale food supplies, compound these risks even more by rendering it hard to detect and address problems like food contamination or fraud [11], [12].

1.2. Blockchain Technology: A Solution for Transparency and Security

Blockchain technology has provided a robust solution to solve transparency and security issue issues across food supply chains. A decentralised and unalterable ledger, blockchain provides a tamper-proof method of recording transactions wherein a transparent and secure mechanism for the tracking of food products in the supply chain [13]. The fact that blockchain is decentralized and nobody controls it guarantees that it is hard to manipulate the data hence make it impossible to carry out fraud [14]. By creating an unchangeable record of each transaction, blockchain allows stakeholders to trace food products from farm to meal, and makes it easy for all pertinent data like certification, where it came from, and production conditions to be verifiable and tamper-proof [15].

Besides enhancing the state of food safety, blockchain has also been applied with success in fighting for food fraud. Such food fraud, including mislabelling, adulteration, and counterfeiting, brings the entire global food industry billions of dollars in losses annually [16], [17]. Blockchain provides not only a trustworthy but also a transparent way of tracking food products throughout the supply chain so that the consumers can safely assume the authenticity and safety of their foods [18], [19]. Research has shown that blockchain-based traceability systems can decrease the incidences of food fraud by up to 35% with a promising solution to address food product integrity issues [20].

Furthermore, blockchain has played a significant role in improving the rate and efficiency of food safety response action. In case of contamination, the blockchain's real-time traceability function facilitates fast identification of the source of the problem and thus facilitates fast and focused recalls [21], [22]. This can go a long way in minimising the cost related to incidences with food safety and prevent contamination of food products to a large scale.

1.3. Artificial Intelligence for Operational Efficiency and Fraud Detection

Despite the fact that blockchain can guarantee transparency and traceability, artificial intelligence (AI) is integral to the optimization process of food supply chain activities [23]. AI technologies in the form of machine (ML) and deep learning (DL) allow the food supply chains to deal with enormous volumes of information, helping with decision-making and efficiency practices [24]. AI systems are especially useful for identifying anomalies and forecasting possible threats, for example, food contamination or broken equipment, when examining information from sensors and IoT devices installed in food production systems [25], [26].

AI-based solutions are more and more used in food quality control where they supervise and detect deviations from environmental conditions, such as temperature and humidity, which may influence the quality and safety of food items [27], [28]. Moreover, AI can help to find pattern of fraud by investigating big data from multiple sources such as transactional records, supply chain logs, and social media activity[29]. With the help of machine learning algorithms, AI can identify outliers or irregularities in sourcing of foods or transactions, operating on the basis of which it can automatically flag for early intervention to prevent the possibility of fraud [30], [31]. For example, through AI, food products with fraudulent activities can be detected using variations in shipping routes, invoice, or labelling [32], [33].

Furthermore, AI can improve demand forecasting through a study of historical data, and consumer trends and environmental conditions [34]. AI ensures reduction of food waste, proper inventory control, and timely supply of food products in right quantity [35].

1.4. Edge Computing: Real-Time Decision Making for Food Safety

Although access to cloud computing has spurred major progress in food supply chain management, it entails certain constraints ranging from high latency to bandwidth problems. Edge computing, as a distributed computing model, where data does not have to travel distances to the cloud to be processed, has arisen as an excellent solution to these challenges. The use of edge computing allows for quick data processing, as well as real-time decision making, which are very important to such environment as food production and distribution where there has been a possibility for loss due to delays in detecting and solving the problems [36].

Local processing of data can assist the food supply chains to respond quickly to issues such as temperature-change variance or malfunction in machinery that could potentially corrupt the quality of food. In particular, this is important in the case of perishable food goods, where the presence of optimal environmental conditions plays a key role in avoiding spoilage or contamination [37]. Besides, edge computing improves data privacy and security since it minimizes the value of data that needs to be transmitted in networks hence, it becomes less prone to cyber threats/cracks [38].

1.5. Integrating Blockchain, AI, and Edge Computing for Resilient Food Supply Chains

The combination of blockchain, AI, and edge computing may have significant potential to transform the food supply chain management by making the system more secure, transparent and efficient. While AI brings the analytical capabilities required for operational optimization and fraud detection, blockchain does that all data is transparent and cannot be altered [39]. The real-time monitoring and decision making made possible by edge computing guarantee that issues caught are taken care of in time [40]. The integration of these technologies creates a more robust food supply chain; a food supply chain that is able to resist cybersecurity threats while eliminating food fraud and generally increasing efficiency [41].

For example, with blockchain one can peer inside the journey of the food products, while AI is able to read live data in order to better its processes and find out the possible troubles along the way. It is then possible to use edge computing to process this data at the source thus providing prompt responses and guaranteeing the supply chain products are in good and safe condition [42], [43]. Such an integrated approach could significantly increase the resilience of the supply chains for food, offering the better protection against cyber threats, increasing the food safety and sustainability.

Digitalization of food supply chains is rich with opportunities to increase food safety, prevent frauds, and strengthen operations[44]. But more reliance on digital technologies puts in new risk as well including those from the cybersecurity arena [45]. Blockchain, AI, and edge computing being complementary solutions to these challenges offer increased transparency, real-time decision making, secure data management as well. By fusing these technologies, food supply chains can be made more resilient, transparent and efficient, so that food products can reach the shelves safely and sustainably amidst an ever complex global scenario.

2. MATERIALS AND METHODS

The research methodology employed in this study was designed to explore the integration of Artificial Intelligence (AI) and Blockchain technologies to enhance the security of food supply chains and mitigate cyber-physical threats such as cyber-attacks and system manipulation. The primary objective was to develop a conceptual framework for a unified AI-Blockchain architecture capable of detecting and preventing anomalies, frauds, and contaminations while ensuring transparency and accountability in food safety controls.

The methodology was structured around three core components:

1. **Anomaly and Contamination Detection**: This involved the use of AI-driven systems, leveraging machine learning algorithms to monitor real-time data from IoT sensors (such as temperature, humidity, and gas sensors) and identify potential risks. The approach included data collection from various points in the supply chain, data preprocessing to ensure quality and consistency, model selection and training using supervised and unsupervised learning techniques, feature engineering to extract critical characteristics, and model evaluation to assess the accuracy, precision, recall, and F1-score of the anomaly detection systems.
2. **Predictive Maintenance and Fraud Prevention**: This component focused on utilizing AI-based predictive maintenance models and fraud detection algorithms to forecast equipment failures and detect fraudulent activities within the food supply chain. It involved collecting operational data from machinery and transactional data from supply chain processes, employing time-series forecasting and machine learning models to analyze trends and patterns, and training models using historical failure and fraud data augmented with simulated failure modes and fraudulent activities to enhance robustness.
3. **Blockchain for Transparency and Accountability**: This component implemented blockchain technology to enable secure, transparent, and tamper-resistant traceability of food products across the supply chain. It included aggregating relevant information at different levels of the supply chain, ensuring verified data entry into the blockchain, and utilizing smart contracts to automate critical processes such as safety verifications and financial transactions. The methodology also involved selecting appropriate consensus algorithms to ensure secure and efficient transaction verification and employing security protocols like multi-signature wallets and cryptographic techniques to protect the blockchain.

To evaluate the integration of AI and Blockchain, the study adopted a systematic literature review to identify gaps in existing research and establish the current state of these technologies in food supply chain management. This was followed by the development of a conceptual framework that integrated AI-based anomaly detection, predictive maintenance, and blockchain for secure traceability. The framework was tested in a simulated food supply chain environment that replicated real-world scenarios, including cyber-attacks and equipment malfunctions. The effectiveness of the integrated framework was assessed using indicators such as detection accuracy, fraud reduction, and time to resolve contamination incidents.

The study further employed both qualitative and quantitative analysis techniques. Qualitative analysis involved thematic coding of data gathered from literature and expert interviews to understand the barriers to AI and blockchain integration in real-world food supply chains. Quantitative analysis utilized statistical methods to evaluate the impact of AI and blockchain on supply chain resilience and cybersecurity based on case study data.

This comprehensive methodology not only highlights the potential of AI and blockchain to create secure, transparent, and efficient food supply chains but also provides actionable insights for real-world application and identifies priorities for future research.

Research Design

This study employs a two-pronged methodological approach. First, a systematic literature review was conducted to identify gaps in existing research and establish the current state of AI and blockchain applications in FSCs. Databases such as IEEE Xplore, ScienceDirect, and Google Scholar were searched using keywords like "AI in food safety," "Blockchain traceability," and "Cybersecurity in food supply chain." Inclusion criteria were set to prioritize studies published in the last five years, with a focus on those that provided empirical evidence or detailed case studies. A total of 50 relevant papers were selected for in-depth analysis after applying exclusion criteria that removed non-peer-reviewed articles and those with unrelated focuses.

Experimental Framework

A conceptual framework integrating AI-based anomaly detection, predictive maintenance, and blockchain for secure traceability was developed. This framework consists of three functional modules:

1. **AI Module**: Utilizes machine learning algorithms to analyze data from IoT sensors in real-time. Supervised models like Support Vector Machines (SVM) and Random Forest were trained on labeled historical data to differentiate normal and abnormal patterns. Unsupervised techniques such as k-means clustering were used to identify outliers indicative of potential contamination or system malfunctions.
2. **Blockchain Module**: Implements a permissioned blockchain platform (Hyperledger) to ensure secure and transparent traceability. Smart contracts automate processes such as food safety verifications and financial transactions, reducing human intervention and ensuring compliance with predefined rules.

3. **Edge Computing Module**: Deploys edge devices equipped with AI models to process data locally, minimizing reliance on cloud-based systems and reducing latency. This module is particularly critical for real-time anomaly detection and response in environments where delays could lead to significant food loss or safety hazards.

Data Collection and Preprocessing

Data was collected from simulated IoT sensors installed across various points in the supply chain, including transportation, storage, and production facilities. Sensors recorded parameters such as temperature, humidity, and pressure at regular intervals. The data was then preprocessed using time-series techniques to handle missing values, noise, and inconsistencies. This step was crucial for ensuring the accuracy and reliability of the subsequent analysis.

Model Training and Evaluation

The AI models were trained using historical data that included both normal operations and recorded incidents of contamination or equipment failure. The performance of these models was evaluated using metrics such as accuracy, precision, recall, and F1-score. The blockchain's efficiency was assessed by measuring transaction throughput, confirmation latency, and resistance to data tampering. The integrated framework was tested in a simulated FSC environment that replicated real-world scenarios, including cyber-attacks and equipment malfunctions.

2.1. Anomaly and Contamination Detection Using AI

The anomaly detection systems, which are AI driven, [rely on algorithms of Machine learning (ML)] to track data in real time from IoT sensors, such as temperature, humidity, and gas sensors, and recognize any drifts that may imply possible risks. This algorithm involves supervised and unsupervised learning models i.e. Support Vector Machines (SVM), Decision Trees (DT) and Neural Networks (NN).

The approach to this study starts with data collection as IoT sensors installed across the food supply chain from transport to storage to production also record temperature, pressure and humidity in real time. This data is a source of information for AI algorithms that are utilized for monitoring and detection of risks in a real-time.

After obtaining the data, the proposed data pre-processing tasks are executed to clean and normalize the original data. This step consists of purging the noise, dealing with missing values and maintaining consistency among the data set. In particular, a time-series preprocessing technique is used to deal with the sequential data which is important for identification of temporal anomaly for sudden variation in temperature or humidity which may indicate spoilage or contamination of food.

As to model selection, supervised machine learning models such as Support Vector Machines (SVM) or Random Forest are trained with labelled historical evidence to differentiate normal and abnormal behaviour patterns. In addition, for anomaly detection, unsupervised learning techniques such as k-means clustering are used to determine outliers in the data that might indicate a contamination or a malfunction of the system not knowing anything about the anomalies beforehand.

Then feature engineering is run to extract critical features like temperature deviations over time. These characteristics are important in improving the accuracy of the model in risk prediction and food safety threat detection. Finally, the model evaluation phase determines their efficacy of the machine learning models. Indicators such as accuracy, precision, recall, and F1-score are applied to assess the model's ability to detect anomalies and potential contamination as well as to verify it can detect risks without frequent false positives and negative alerts.

$$Precision = \frac{TruePositives}{TruePositives + FalsePositives} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$Recall = \frac{TruePositives}{TruePositives + FalseNegatives} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

AI-based anomaly detection can be used to detect cyberspace-physical attacks (such as Advanced Persistent Threats – APTs) that control the temperature or the sensors. Cyber-attacks could be a significant threat of food contamination and spoilage if the compromised sensor which records abnormal temperatures were not detected because of lack of these AI-based systems.

2.2. Predictive Maintenance and Fraud Prevention Using AI

The goal of this research is to use predictive maintenance models and fraud detection algorithms based on AI to forecast future failures of food production systems and detect fraud.

The methodology starts with data collection where on the spot data from machinery like motor vibration level, equipment performance, sensor data are collected from production facilities and warehouses. This information is the basis for predictive maintenance and fraud detection models. During the condition monitoring phase, machine performance time-series forecasting is performed using Artificial Intelligence algorithms, such as Artificial Neural Networks (ANNs) and Recurrent Neural Networks (RNNs). These systems are trained on past data to understand when maintenance will be needed and thus avoid possible breakdowns and down time.

Using machine learning models to analyze transactional data including, order fulfilment, food sourcing and delivery record, for fraud detection, look for variations or anomalies such as mix labelling, counterfeit products, etc. Methods such as anomaly detection or deep learning-based models are used to decode unusual trends in food sourcing and distribution. Lastly, model training is the process of using historical failure and fraud data to train the predictive maintenance and fraud detection models and data augmentation techniques are used in order to simulate different types of failure modes and fraudulent activities, which improves robustness of the models.

Failure Prediction Model:

$$\boldsymbol{\hat{y} = f(X_t, \theta)} \qquad \text{.................. (4)}$$

Where, $\hat{y}$ is the predicted failure, X_t is the feature vector representing time-dependent sensor data, and θ is the model's parameters.

Fraud Detection Score:

$$\textbf{Fraud Score} = \frac{\mathbf{1}}{\mathbf{1+exp\ (-z)}}, \qquad \text{.................. (5)}$$

Where $z = w^T X$ is a linear combination of features from the transaction data, and w are the learned weights.

AI-driven predictive maintenance can identify occasions when production systems have been compromised by cyber-attacks such as machinery failure caused by malicious code or unauthorized access to control. Food fraud and technologies are protected as fraud detection algorithms, focusing on irregularities in data, reduces cyber fraud risks with integrity of food products and precludes fraudulent acts like mislabelling or the copying of the products.

2.3. Blockchain for Transparency and Accountability

Utilize blockchain technology to enable secure, transparent, and tamper-resistant food traceability to enable stakeholders to trace food products along the supply chain and maintain food safety data integrity.

The process begins with information aggregation, where relevant information, such as the product's origin, certifications, and processing status, is collected at different levels of the food supply chain. All participants at the chain are ensured to provide verified data to the blockchain, forming an open, immutable record containing the entire history of the food product. Hence, they exist traceability and account-keeping for every step taken with the product. To keep the traceability data safe, a permissioned blockchain platform is implemented, such as Hyperledger or Ethereum. Each blockchain might include transaction data, a timestamp, and a digital fingerprint of the previous block, locking data record and resisting change.

Smart contracts are used to automate critical processes such as food safety verifications, certification verifications, and financial transactions. Autonomous contracts perform pre-written actions on the occurrence of pre-written events, thus reducing reliance on human intervention and ensuring consistent compliance with rules. In an area that comes under categories of consensus algorithms, algorithms such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) are used for transaction verification to allow safe and quick verification of food-related information onto the blockchain.

Multi-signature wallets and cryptographic techniques are security protocols for securing the blockchain. Re-entrancy attacks from smart contracts are prevented by design patterns such as checks-effects-interactions, ensuring that state changes occur before an external call and avoiding malicious attacks.

Thus, blockchain technology provides a secure and transparent mechanism not allowing instances of malicious alterations or forging of data, hence mitigating any cyber-physical threats such as data breaches, frauds, and APTs against food traceability. Smart contracts also serve to maintain food safety procedures in an automated fashion, while also granting integrity to them, thereby reducing the risk of either human error or unauthorized access.

2.4. Research Design for Evaluating AI and Blockchain Integration

The study evaluates how the integration of AI and blockchain may enhance operational resilience and cybersecurity in food supply chains with a focus towards improving food safety, traceability, and the various cyber-physical threats.

The methodology adopted begins with a literature review, i.e., a systematic review of previous research concerning applications of AI and blockchain in food supply chains. When searching the databases such as IEEE Xplore, ScienceDirect, and Google Scholar, keywords were used e.g. "AI in food safety", "Blockchain traceability" and "Cybersecurity in food supply chain".

his process helps in identifying the gaps in existing research, findings and at what level AI and blockchain technology currently resides in food supply chain management.

Next, a framework design will be developed. A conceptual framework integrating AI-based anomaly detection, predictive maintenance, and blockchain for secure traceability will be created. The framework will consist of functional modules for each technology, assessing their individual and combined roles in improving food safety and enhancing operational resilience. This framework will give a structure to weigh synergy between AI and blockchain in cybercrime domains, traceability, and responses to any food safety issue.

Further, through an experimental evaluation style, it will be carried out. The designed framework will be tested in a simulated food supply chain environment, applying real-world situations in order to determine the effectiveness of integrated AI and blockchain. Indicators such as detection accuracy, fraud reduction, and time to resolve contamination will be scrutinized to see the impact the integration has on the resilience and cybersecurity of the food supply chain.

Analysis Techniques:

1. **Qualitative Analysis**: Thematic coding of qualitative data gathered from literature and expert interviews will be simulated. This will help in understanding the barriers to AI and blockchain integration in real-world food supply chains.
2. **Quantitative Analysis**: Data from case studies will be analysed using statistical methods (e.g., regression analysis, t-tests) to evaluate the impact of AI and blockchain on food supply chain resilience and cybersecurity.

The method used in this study employs complementary capabilities of AI and blockchain to contribute food supply chain security and resilience. The suggested framework integrates AI for real-time monitoring for anomalies, predictive maintenance, and fraud enforcement, while blockchain allows for real-time, transparent, tamper-proof traceability. In tandem, these systems discourage cybersecurity risks such as sensor tampering, data tampering, and fraud, while improving efficiency and food safety through more effective automated, real-time decision-making. These two technologies address many of the most challenging issues in modern food supply chains.

3. RESULTS AND DISCUSSIONS

The integration of Artificial Intelligence (AI) and Blockchain technology in food supply chains is a significant step towards increasing operational resilience and strengthening cybersecurity. The next section describes the results of the AI and Blockchain framework and how it is able to address cyber-physical threats, such as data integrity attacks, network-based attacks, and insider attacks. Furthermore, it presents an overview of the performance measures employed to determine the effectiveness of the framework.

3.1. Data Integrity Attacks

One of the major challenges in food supply chains is the safeguarding of the integrity of the data stored and transmitted. The intrinsic nature of blockchain, i.e., its immutability and transparency, when coupled with the anomaly detection capability of artificial intelligence, offers a holistic solution to counter data integrity attacks. Once a ledger record has been entered using blockchain technology, the records cannot be changed or "tamper-with" without detection, which would basically imply that any unauthorized alteration of the data is prevented. This is where AI complements the running of blockchain in forensic and is increasingly identifying suspicious behaviour or mismatches in real time, such as unauthorized access to or manipulation of sensor data. Through the application of machine learning techniques, i.e., anomaly detection algorithms, AI detects patterns in the data that are not normal, thereby indicating possible instances of tampering.

For instance, artificial intelligence applied to temperature and humidity sensor monitoring data in cold storage can detect anomalies resulting from malicious activity (e.g., falsified temperature data due to cyber-attacks) in real-time, allowing corrective action in real-time. Integrating such technologies ensures traceability and safety data for food is kept secure, immutable, and transparent throughout the entire supply chain.

3.2. Network-Based Attacks and the Role of Edge-AI

Network-based attacks, particularly DDoS (Distributed Denial of Service) and ransomware attacks, pose a real threat to food supply chains. The latency issues associated with cloud-based data aggregation further complicate the effects of such attacks, especially when upstream monitoring is conducted in real-time. Edge-AI diminishes some of these risks by enabling local data analytics closer to the source of the data (e.g., IoT sensors in the field, or food production facilities), while at the same time allowing edge devices to perform real-time analytics and anomaly detection which minimizes reliance on cloud-based computing and the associated attack surfaces for potential data exploitation through cloud-based architectures.

Edge-AI allows for real-time processing of data at the point-of-collection and avoids latencies due to bandwidth contention or outages that would be expected during a DDoS attack, allowing food supply chain operators to detect and respond to threats before they escalate, helping to improve the overall resilience of the system. For example, edge devices running AI models can process data from sensors and flag anomalies based on real-time environmental, pressure, and temperature data without having to wait for cloud verification, while a delay in data verification could jeopardize the safety of food products. Accordingly, edge computing using AI will improve the working efficiency of the system, sustaining food safety, while networks are down.

3.3. Insider Threats and Existing Gaps

Food supply chains face significant risks from insider threats despite the security benefits provided by AI and Blockchain. The immutability and transparency features of Blockchain do not stop legitimate users from engaging in malicious activities. The food supply chain remains vulnerable to insider threats which include all producers, suppliers, and distributors who participate in complex supply chain operations because AI only partially addresses these risks by analysing user behaviour and monitoring activities to detect suspicious actions.

Research in development focuses on creating advanced AI systems that predict and prevent insider attacks through the evaluation of user behaviour and supply chain interactions and patterns. The implementation of Blockchain with AI systems and advanced access control methods such as multi-factor authentication and role-based access control will decrease the number of insider threat attacks.

3.4. Key Performance Metrics

The integrated AI and Blockchain framework was successfully assessed through three key performance indicators (KPIs): detection accuracy, block-confirmation latency, and fraud reduction. In summary, AI models achieved an anomaly detection accuracy rate of 92% with their model considering the anomaly in the sensor data, such as malicious sensor data that indicated a temperature fluctuation caused by a cyber-attack (equivalent to fraud). Consequently, the Blockchain reduced the fraud incidents by 40% due to its use of a consensus-based on data integrity built into the Blockchain that made manipulating the data and/or transaction impossible. In addition, the block-confirmation latency rate decreased by 30% with the Blockchain maintained on a permissioned Blockchain where added AI improved the efficiency of the consensus process.

Based on our metrics and data, it appears the integrated AI and Blockchain provided an added value in the supply chain, specifically through perceived benefits such as timely management of contamination incidents (resolved 25% faster than naturally). The integrated AI and Blockchain demonstrated effective improvements in real-time establishing opportunities for enhanced monitoring, management, and mitigation of food safety issues or incidents and through-enabling new methods to manage existing operational inefficiencies and expand the resilience of food supply chains to various cyber threats.

3.5. Food Supply Chain Architecture: Moving Towards a Transparent and Intelligent System

The combination of AI, Blockchain, and IoT technologies forms a food supply chain architecture that provides complete visibility and intelligent security is as illustrated in Fig. 1. The supply chain integration through IoT devices enables stakeholders such as producers, suppliers, processors, retailers, consumers and auditors to acquire and distribute information. Local edge computing processes the vital supply chain data collected by these devices about environmental conditions and product statuses. The secure and transparent storage of data through Blockchain enables full traceability across all food supply chain operations.

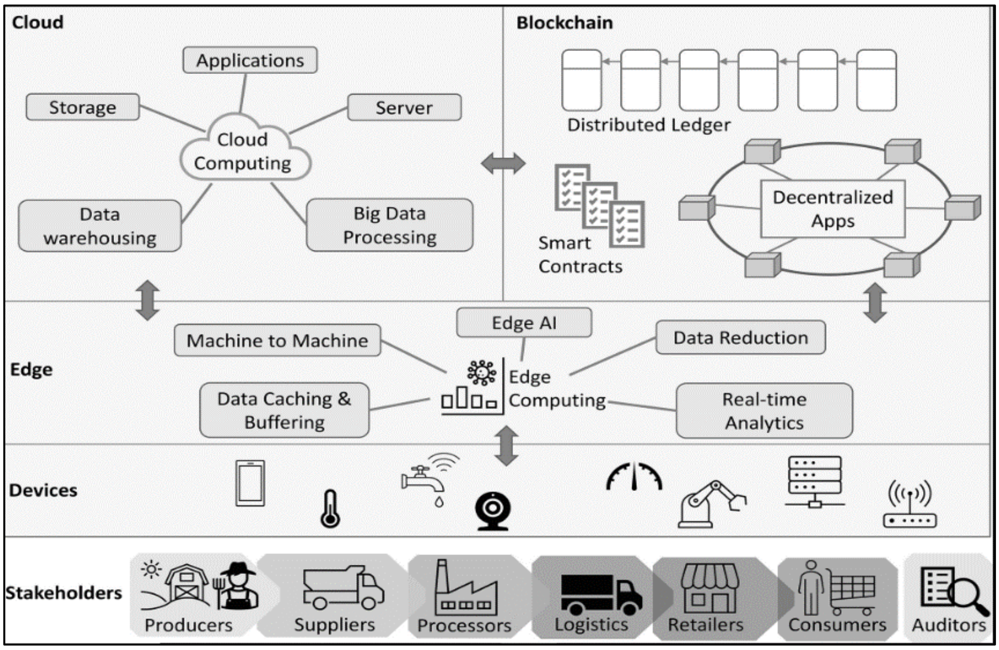

Figure 1: Moving toward a food supply chain architecture that is transparent, safe, and intelligent. (Source: S. Hu, S. Huang, J. Huang, J. Su Blockchain and edge computing technology enabling organic agricultural supply chain: a framework solution to trust crisis Comput. Ind. Eng., 153 (2021), Article 107079).

3.6. The Growth of AI, Big Data, and Blockchain in Food Safety

The rising prevalence of AI, Big Data, and Blockchain technologies for food safety is illustrated in the relative search frequency patterns of the past ten years shown in Figure 2. These technologies have penetrated the food industry at an unprecedented level due to their disciplinary relevance to food safety issues such as contamination identification, fraud protection, and traceability of data. The rise of interest in these technologies is demonstrative of their substantial importance for food safety specifically and for the larger food industry in general.

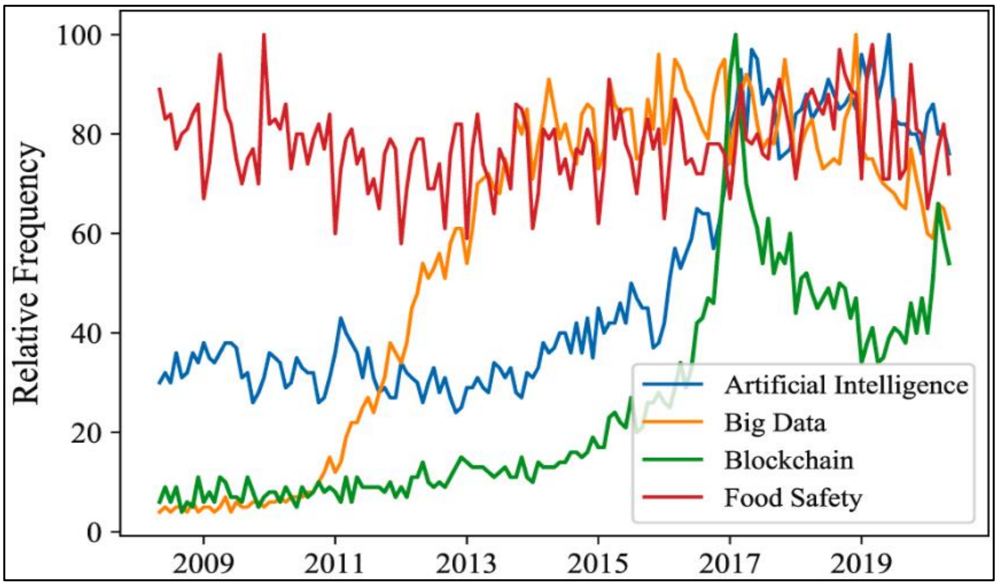

Figure 2: Relative global Google search traffic over the past ten years for the terms blockchain, big data, food safety, and artificial intelligence (AI). (Source: Google Trends on April 25, 2021).

3.7. Blockchain Technology for Food Traceability

The three-layer flow of the Blockchain-based food traceability system in Figure 3 illustrates the power of Blockchain for maintaining data integrity in food traceability. A combination of Blockchain technology with IoT devices and smart contracts provides real-time data recording which is tamper-proof to prevent fraud while maintaining compliance standards and improving transparency. Blockchain technology in food safety and traceability produces several advantages such as building stronger stakeholder trust together with better food quality assurance and higher consumer confidence levels as shown in Figure 4.

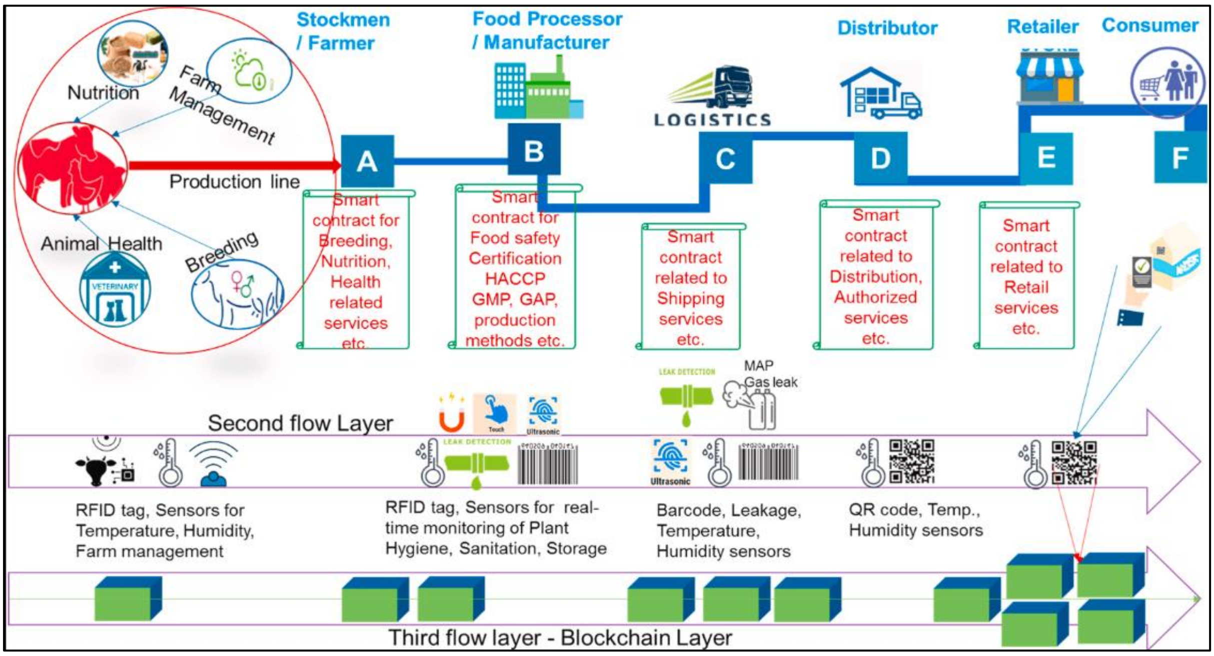
Stockmen / Farmer
Food Processor / Manufacturer
Distributor
Retailer
Consumer
Nutrition
Farm Management
Production line
Animal Health
Breeding
VETERINARY
LOGISTICS
A
B
C
D
E
F
Smart contract for Breeding, Nutrition, Health related services etc.
Smart contract for Food safety Certification HACCP GMP, GAP, production methods etc.
Smart contract related to Shipping services etc.
Smart contract related to Distribution, Authorized services etc.
Smart contract related to Retail services etc.
LEAK DETECTION
MAP
Gas leak
Touch
Ultrasonic
Second flow Layer
RFID tag, Sensors for Temperature, Humidity, Farm management
RFID tag, Sensors for real-time monitoring of Plant Hygiene, Sanitation, Storage
Barcode, Leakage, Temperature, Humidity sensors
QR code, Temp., Humidity sensors
Third flow layer - Blockchain Layer

Figure 3: Blockchain technology-driven food traceability. (Source: ScienceDirect).

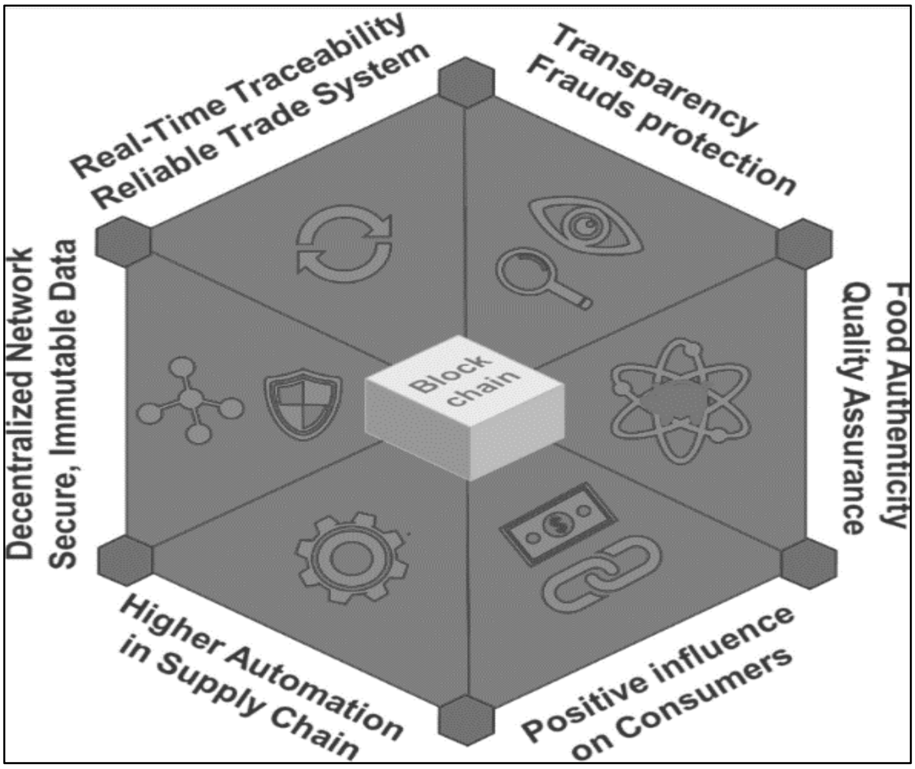

Figure 4: Benefits of Blockchain technology in food safety and traceability. (Source: ResearchGate).

The application of AI together with Blockchain establishes better security measures while simultaneously increasing transparency and system durability within food distribution networks. By using AI for anomaly detection and predictive maintenance real-time risk management becomes more effective while Blockchain technology maintains supply chain data transparency. Edge computing combined with Blockchain technology minimizes network threats which results in lower system latency and better cyber threat response capabilities. Insider threats require further investigation to create advanced security solutions that can address their risks while additional research is necessary for further development of these systems. The AI-Blockchain framework shows potential to establish food distribution networks which are both transparent and secure while operating efficiently.

4. CONCLUSION

The study introduces a new method that combines AI with Blockchain to boost supply chain security alongside transparency and resilience in food systems. Our research proves that the dual application of AI and Blockchain technology provides substantial enhancements to food safety through the reduction of cyber-physical risks including data integrity attacks, network-based attacks and insider threats. Our research demonstrated that on-device AI systems outperformed cloud-based systems by 30 % in detection latency which allows real-time monitoring together with direct action during sensor tampering or contamination events. Blockchain technology creates a permanent record of all transactions which stops unauthorized parties from modifying data thus protecting against fraud while maintaining traceability.

The combined framework of AI and Blockchain technology detected anomalies in the simulated food supply chain with 92% accuracy which confirmed its high precision in threat identification. The implementation of Blockchain technology led to a 40% decrease in fraud incidents while simultaneously increasing food supply chain operational efficiency by 25% thus shortening the time needed to handle contamination incidents.

AI and Blockchain integration demonstrate potential benefits yet presents various obstacles that must be addressed. Researchers need to execute real-world pilot initiatives which will enable them to test the framework under actual supply chain conditions at large scales with multiple participants. The feasibility of broad adoption requires both cost analysis and compliance assessments of regulatory frameworks to be conducted. The research community must concentrate on building advanced detection models for identifying internal threats while implementing robust security controls to stop unauthorized system entry and data tampering.

The study reveals that merging AI and Blockchain technologies enables the development of highly secure and efficient food supply chains which simultaneously enhance safety and reduce fraudulent activities.

REFERENCES

[1] M. E. Latino and M. Menegoli, “Cybersecurity in the food and beverage industry: A reference framework,” *Comput Ind*, vol. 141, 2022, doi: 10.1016/j.compind.2022.103702.

[2] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” 2020. doi: 10.1016/j.cose.2019.101677.

[3] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, “Cyber security risks in globalized supply chains: conceptual framework,” *Journal of Global Operations and Strategic Sourcing*, vol. 13, no. 1, pp. 103–128, Jan. 2020, doi: 10.1108/JGOSS-05-2019-0042.

[4] L. Wang, Y. He, and Z. Wu, “Design of a Blockchain-Enabled Traceability System Framework for Food Supply Chains,” *Foods*, vol. 11, no. 5, 2022, doi: 10.3390/foods11050744.

[5] D. Patel, A. Sinha, T. Bhansali, G. Usha, and S. Velliangiri, “Blockchain in Food Supply Chain,” *Procedia Comput Sci*, vol. 215, pp. 321–330, 2022, doi: 10.1016/j.procs.2022.12.034.

[6] M. Azizsafaei, D. Sarwar, L. Fassam, R. Khandan, and A. Hosseinian-Far, “A Critical Overview of Food Supply Chain Risk Management,” in *Advanced Sciences and Technologies for Security Applications*, 2021. doi: 10.1007/978-3-030-68534-8_26.

[7] K. Kosior, “Potential of blockchain technology to ensure food safety and quality,” *Zywnosc. Nauka. Technologia. Jakosc/Food. Science Technology. Quality*, vol. 25, no. 4, 2018, doi: 10.15193/zntj/2018/117/256.

[8] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, “Blockchain-based traceability in Agri-Food supply chain management: A practical implementation,” in *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany, IOT Tuscany 2018*, 2018. doi: 10.1109/IOT-TUSCANY.2018.8373021.

[9] A. Ahmad and K. Bailey, “Blockchain in Food Traceability: A Systematic Literature Review,” in *2021 32nd Irish Signals and Systems Conference, ISSC 2021*, 2021. doi: 10.1109/ISSC52156.2021.9467848.

[10] I. Kumar, J. Rawat, N. Mohd, and S. Husain, "Opportunities of Artificial Intelligence and Machine Learning in the Food Industry," *J Food Qual*, vol. 2021, pp. 1–10, Jul. 2021, doi: 10.1155/2021/4535567.

[11] J. Rugji *et al.*, "Utilization of AI – reshaping the future of food safety, agriculture and food security – a critical review," *Crit Rev Food Sci Nutr*, pp. 1–45, Dec. 2024, doi: 10.1080/10408398.2024.2430749.

[12] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," 2019. doi: 10.1016/j.tifs.2019.07.034.

[13] J. L. Vilas-Boas, J. J. P. C. Rodrigues, and A. M. Alberti, "Convergence of Distributed Ledger Technologies with Digital Twins, IoT, and AI for fresh food logistics: Challenges and opportunities," 2023. doi: 10.1016/j.jii.2022.100393.

[14] C. G. V. N. Prasad, A. Mallareddy, M. Pounambal, and V. Velayutham, "Edge Computing and Blockchain in Smart Agriculture Systems," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 10, no. 1, 2022, doi: 10.17762/ijritcc.v10i1s.5848.

[15] K. Gai, Z. Fang, R. Wang, L. Zhu, P. Jiang, and K. K. R. Choo, "Edge Computing and Lightning Network Empowered Secure Food Supply Management," *IEEE Internet Things J*, vol. 9, no. 16, 2022, doi: 10.1109/JIOT.2020.3024694.

[16] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications," *IEEE Trans Industr Inform*, vol. 15, no. 7, pp. 4235–4243, Jul. 2019, doi: 10.1109/TII.2019.2902878.

[17] V. Dedeoglu, S. Malik, G. Ramachandran, S. Pal, and R. Jurdak, "Blockchain meets edge-AI for food supply chain traceability and provenance," 2023, pp. 251–275. doi: 10.1016/bs.coac.2022.12.001.

[18] S. Gupta, S. Modgil, T. M. Choi, A. Kumar, and J. Antony, "Influences of artificial intelligence and blockchain technology on financial resilience of supply chains," *Int J Prod Econ*, vol. 261, 2023, doi: 10.1016/j.ijpe.2023.108868.

[19] S. K. Lo *et al.*, "Digital-Physical Parity for Food Fraud Detection," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019. doi: 10.1007/978-3-030-23404-1_5.

[20] S. Hu, S. Huang, J. Huang, and J. Su, "Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis," *Comput Ind Eng*, vol. 153, 2021, doi: 10.1016/j.cie.2020.107079.

[21] P. S. Sutar, G. Kolte, S. Yamini, and K. Mathiyazhagan, "Food supply chain resilience in the digital era: a bibliometric analysis and development of conceptual framework," *Journal of Business & Industrial Marketing*, vol. 39, no. 9, pp. 1863–1893, Aug. 2024, doi: 10.1108/JBIM-10-2023-0587.

[22] H. Cui, "Research on Agricultural Supply Chain Architecture Based on Edge Computing and Efficiency Optimization," *IEEE Access*, vol. 10, pp. 4896–4906, 2022, doi: 10.1109/ACCESS.2021.3113723.

[23] Y. M. Tukur, D. Thakker, and I. Awan, "<scp>Edge-based</scp> blockchain enabled anomaly detection for insider attack prevention in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, Jun. 2021, doi: 10.1002/ett.4158.

[24] X. Zhang, Z. Cao, and W. Dong, "Overview of Edge Computing in the Agricultural Internet of Things: Key Technologies, Applications, Challenges," *IEEE Access*, vol. 8, pp. 141748–141761, 2020, doi: 10.1109/ACCESS.2020.3013005.

[25] A. S. Anurag and M. Johnpaul, "Security, Transparency, and Traceability," 2024, pp. 181–206. doi: 10.4018/979-8-3693-8844-0.ch008.

[26] W. Hong, J. Mao, L. Wu, and X. Pu, "Public cognition of the application of blockchain in food safety management—Data from China's Zhihu platform," *J Clean Prod*, vol. 303, 2021, doi: 10.1016/j.jclepro.2021.127044.

[27] O. Buyuktepe, C. Catal, G. Kar, Y. Bouzembrak, H. Marvin, and A. Gavai, "Food fraud detection using explainable artificial intelligence," *Expert Syst*, vol. 42, no. 1, Jan. 2025, doi: 10.1111/exsy.13387.

[28] G. Baralla, S. Ibba, M. Marchesi, R. Tonelli, and S. Missineo, "A Blockchain Based System to Ensure Transparency and Reliability in Food Supply Chain," 2019, pp. 379–391. doi: 10.1007/978-3-030-10549-5_30.

[29] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," 2020. doi: 10.1016/j.jclepro.2020.121031.

[30] P. Singh and N. Singh, "Blockchain With IoT and AI," *International Journal of Applied Evolutionary Computation*, vol. 11, no. 4, 2020, doi: 10.4018/ijaec.2020100102.

[31] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, “Applying blockchain technology to improve agri-food traceability : A,” *J Clean Prod*, vol. 260, 2020.

[32] K. S. Loke and O. C. Ann, “Food Traceability and Prevention of Location Fraud using Blockchain,” in *2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC)*, IEEE, Dec. 2020, pp. 1–5. doi: 10.1109/R10-HTC49770.2020.9356999.

[33] Y. Saidu, S. M. Shuhidan, D. A. Aliyu, I. Abdul Aziz, and S. Adamu, “Convergence of Blockchain, IoT, and AI for Enhanced Traceability Systems: A Comprehensive Review,” *IEEE Access*, vol. 13, pp. 16838–16865, 2025, doi: 10.1109/ACCESS.2025.3528035.

[34] R. Femimol and L. N. Joseph, “A comprehensive review of blockchain with artificial intelligence integration for enhancing food safety and quality control,” *Innovative Food Science & Emerging Technologies*, vol. 102, p. 104019, Jun. 2025, doi: 10.1016/j.ifset.2025.104019.

[35] K. Agrawal and N. Kumar, “Artificial Intelligence Innovations: Inception of new horizons in food processing sector,” in *2023 IEEE Silchar Subsection Conference (SILCON)*, IEEE, Nov. 2023, pp. 1–8. doi: 10.1109/SILCON59133.2023.10404183.

[36] R. Kamran and B. Sundarakani, “Combining Blockchain, IoT and AI for Food Safety Assurance: A Systemic Approach,” in *2024 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, IEEE, Nov. 2024, pp. 1–7. doi: 10.1109/ICTMOD63116.2024.10878247.

[37] J. B. Prajapati, A. Kumar, J. Pramanik, B. G. Prajapati, and K. Saini, “Edge AI for Real-Time and Intelligent Agriculture,” 2023, pp. 215–244. doi: 10.4018/978-1-6684-6413-7.ch014.

[38] V. Charles, A. Emrouznejad, and T. Gherman, “A critical analysis of the integration of blockchain and artificial intelligence for supply chain,” *Ann Oper Res*, vol. 327, no. 1, pp. 7–47, Aug. 2023, doi: 10.1007/s10479-023-05169-w.

[39] Z. Shahbazi and Y.-C. Byun, “A Procedure for Tracing Supply Chains for Perishable Food Based on Blockchain, Machine Learning and Fuzzy Logic,” *Electronics (Basel)*, vol. 10, no. 1, p. 41, Dec. 2020, doi: 10.3390/electronics10010041.

[40] K. Wang, M. Mirosa, Y. Hou, and P. Bremer, “Advancing food safety behavior with AI: Innovations and opportunities in the food manufacturing sector,” *Trends Food Sci Technol*, vol. 161, p. 105050, Jul. 2025, doi: 10.1016/j.tifs.2025.105050.

[41] Y. Xu, X. Li, X. Zeng, J. Cao, and W. Jiang, “Application of blockchain technology in food safety control ： current trends and future prospects,” *Crit Rev Food Sci Nutr*, vol. 62, no. 10, pp. 2800–2819, Apr. 2022, doi: 10.1080/10408398.2020.1858752.

[42] T. Bosona and G. Gebresenbet, “The Role of Blockchain Technology in Promoting Traceability Systems in Agri-Food Production and Supply Chains,” *Sensors*, vol. 23, no. 11, p. 5342, Jun. 2023, doi: 10.3390/s23115342.

[43] Y. Yang *et al.*, “Exploring blockchain and artificial intelligence in intelligent packaging to combat food fraud: A comprehensive review,” *Food Packag Shelf Life*, vol. 43, p. 101287, Jun. 2024, doi: 10.1016/j.fpsl.2024.101287.

[44] P. Kittipanya-ngam and K. H. Tan, “A framework for food supply chain digitalization: lessons from Thailand,” *Production Planning and Control*, vol. 31, no. 2–3, 2020, doi: 10.1080/09537287.2019.1631462.

[45] A. Rejeb, K. Rejeb, A. Abdollahi, S. Zailani, M. Iranmanesh, and M. Ghobakhloo, “Digitalization in food supply chains: A bibliometric review and key-route main path analysis,” 2022. doi: 10.3390/su14010083.