AI-Powered Food Freshness Detection with Blockchain-Based Product Authentication.

By

Saiful Islam Sumon
221-15-5664

Md. Shahinur Alam Rabbi
221-15-4673

FINAL YEAR DESIGN PROJECT REPORT

This Report Presented in Partial Fulfillment of the Requirements forthe **Degree of Bachelor of Science in Computer Science and Engineering**

Supervised by

Ms. Syeda Tasmia Alvi

Senior Lecturer
Department of Computer Science and EngineeringDaffodil International University

Co-Supervised by

Mr. Md Assaduzzaman

Assistant Professor
Department of Computer Science and EngineeringDaffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

Dhaka, Bangladesh

APPROVAL

This Project titled **"AI-Powered Food Freshness Detection with Blockchain-Based Product Authentication"** submitted by **Saiful Islam Sumon** and **Md. Shahinur Alam Rabbi** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science andEngineering and approved as to its style and contents. The presentation has been held on **7-1-2026**.

BOARD OF EXAMINERS

Dr. Md Ali Hossain
Board Chairman
Associate Professor, Chairman,
Department of CSE, FSIT, Daffodil
International University

7/1/26

Ms Syeda Tasmia Alvi
Internal Examiner 1
Senior Lecturer, Department of
CSE, FSITDaffodil International
University

07.01.26

Mr Md. Ashaf Uddaula
Internal Examiner 2
Lecturer, Department of CSE, FSIT
Daffodil International University

Dr. Selina Sharmin
External Examiner
Professor
Department of CSE,
Jagannath University

DECLARATION

We hereby declare that this project has been done by us under the supervision of **Ms. Syada Tasmia Alvi, Senior Lecturer,** Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this projectnor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Alvi 7/1/26

Ms. Syada Tasmia Alvi
Senior Lecturer
Department of Computer Science and Engineering, Daffodil International University

Co-Supervised by:

Mr. Md Assaduzzaman
Assistant Professor
Department of Computer Science and Engineering, Daffodil International University

Submitted by:

Sumon

Saiful Islam Sumon
Student ID: 221-15-5664
Department of Computer Science and Engineering
Daffodil International University

Shahin

Md. Shahinur Alam Rabbi
Student ID: 221-15-4673
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENTS

This work would not have been possible without the support and contributions of many individuals over the past two semesters. We are deeply grateful to everyone who has assisted us in one way or another.

First, we express our heartfelt thanks and gratefulness to the almighty for His divine blessing making it possible for us to complete the **Final Year Design Project(FYDP)** successfully.

We are grateful and wish our profound indebtedness to **Ms. Syada Tasmia Alvi**, **Senior Lecturer**, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh. Deep knowledge and keen interest of our supervisor in the field of **Blockchain** & **Artificial Intelligence** to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting themat all stages have made it possible to complete this project.

We would like to express our heartfelt gratitude to the Head of the Department of Computer Science and Engineering, for his kind help in finishing our project and also to other faculty members and the staff of the Department of Computer Science and Engineering, Daffodil International University.

We would like to thank our entire coursemates at Daffodil International University, who took part in this discussion while completing the coursework.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

ABSTRACT

In the modern setting, Artificial Intelligence and Blockchain technology play a particularly critical and pivotal role in ensuring food supply chain transparency, integrity, and food authentication. Within the developing nations, there are also alarming issues linked to the adulteration of food, the existence of counterfeit food packages in the market, and the inability of the ordinary consumer to determine the freshness of the packaged food. This is in addition to food being inspected in a manual, opaque, and unreliable manner. In view of aforementioned challenges, this research paper proposes an AI and Blockchain-based combined model for improving food safety, authentication, and freshness assessment. This research paper is composed of two main parts, including AI food freshness assessment and food authentication through Blockchain technology. Within the AI module, models made up of Long Short-Term Memory (LSTM) algorithms combined with XGBoost and Random Forest algorithms are trained on a set curated dataset comprising images of fresh as well as rotten foods for accurate classification. Additionally, for packaged foods, a smart contract has been designed on the Ethereum Sepolia test network to securely store the necessary product information such as product number, name, brand name, date of manufacturing, date of expiration, as well as product images held on IPFSA QR code built using the SHA-256 hash connects a physical product directly to the corresponding entry in the blockchain, enabling "customers to instantly authenticate the item's authenticity." By being MetaMask and Web3-compliant, "Only authorized vendors can list the items into the database," increasing the security of the decentralized system. From the experiments performed in the paper, the combination of AI and the use of the "blockchain prevents the entry of counterfeit items into the food supply chain." A "decentralized image hosting solution from the InterPlanetary File System" prevents data breaches in the central server by protecting images from being "manipulated in the process of being stored in the central server."

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter provides the setting of the thesis as a whole and presents issues related to food adulteration, counterfeiting, and food chain transparency. The potential for AI, Blockchain technology, and food storage technologies will also be introduced as a means of addressing food safety and food authenticity. The thesis will then conclude with the thesis report framework.

1.1 Introduction

However, there has been a recent shift in thought with regards to a major change in the current food chain network because of the latest technological advancements available to us. However, food fraud and spreading counterfeited packaging are still a health issue in several developing nations because of weak enforcement by governments. Consumers are often left with no choice but to purchase goods with fraudulently labeled expiration dates, trademarks, and chemically labeled food that looks fresh but isn't actually safe to eat. Food safety is also a major concern in the current scenario, with tainted food items causing illnesses to millions of people around the globe [4], in addition to annual economic costs [11]. The conventional system for traceability in food items is either in the form of paper documentation or a central database, which is prone to tampering, information isolation, and product recalls [4]. There has been some advancement in the application of artificial intelligence (AI) in the related areas of freshness analysis and risk analysis. The most dominant set of literature available in the present scenario emphasizes the applications of powerful Convolutional Neural Networks, which require large amounts of labeled images in the training set and have the limitation of interpretability [2]. Moreover, the applicability in the current scenario is often hindered by the algorithms' exposure to data quality and availability issues [1]. The underlying technology in the current scenario is the ability to maintain immutable and decentralized ledgers, which can enable tamper-proof chain-of-ownership throughout the entire food chain [4]. However, the current underlying infrastructure is mainly in the form of private blockchains that require intense investment in physical infrastructure, as well as scalability issues [8]. In fact, the efficient implementation of food safety technology requires a clear understanding of regulatory issues, since infrastructural constraints have continued to hinder existing technologies [9]. The blockchain approach emerges as a paradigmatic change in this respect, since it is known to enhance traceability in food chains, although regulatory issues have continued to emerge as the main obstacles for implementation [3]. According to systematic reviews, the key evidence available shows that the great majority of food safety practices with blockchain technology have reached the concept-proof stage due to long-standing barriers of cost, compatibility, and alignment with regulations [5]. "Access to qualified parties with blockchain enables users to ensure food product information securely from any site through the blockchain network without depending on any third-party service provider" [20]. To fill these differences, we propose a publicly accessible Ethereum network in which vendors use MetaMask to upload product metadata (product name, brand, date of manufacture and expiration, and images). The multimedia files are moved off-chain through IPFS and a QR code is produced containing the IPFS CID. The buyer can use the QR code to confirm the unalterable record on the blockchain. Removing large amounts of information from the blockchain reduces gas costs to a nominal rate of 0.03 USD per registration and eliminates the expense of the Raft consensus hardware used in the private chains [8]. At the same time, we use light and interpretable models (RF/XGB/LSTM) that combine heterogeneous sensor inputs from the IoT ecosystem by addressing the black box problem of models using CNNs solely [2].In this paper, the authors develop a comprehensive AI blockchain framework that is not only scalable and economically viable but also easy to use to improve the food item's safety. From the findings presented in the past studies that highlighted the lack of effectiveness and sustainability in the current processes being used to check the freshness and reduce the counterfeit goods in the market, this paper hopes to improve consumer practices and supply chain security through the use of technology.

1.2 Motivation

Food safety and authenticities have become more prominent in the current supply chain scenario due to the increasing levels of adulteration and food fraud. Consumers tend to perceive the freshness levels of the food items through a visual assessment or a label in many scenarios. This is particularly vulnerable and prone to fraud. At the moment, the supply chain tracing is highly centralized. Product information can be manipulated and the freshness also depends on some external factors such as temperature, preservation etc.

Moreover, the recent advancements in artificial intelligence have shown significant potential for the automation of visual inspection tasks, particularly through the use of deep learning models to assess the freshness of food by interpreting food images. However, the predictive outcomes from artificial intelligence solutions are inadequate to ensure the authenticity of information related to the product, including its origin, brand, or expiration dates. On the other hand, blockchain technology ensures the integrity of storage but lacks the capability to assess the status of the food items. It can give immutable, secure and transparent product authentication system.

A primary intention of this research work is therefore the development of a hybrid model that incorporates concurrent operations of AI-driven freshness evaluation and blockchain-based authentication for product authenticity, each solving for the limitations of the other. Consumer can scan QR images to fetch product information from blockchain and get images stored in IPFS storage, they can ensure about the product authenticity an no one can manipulate these data. With its ability to validate product information through QR-code entries on a decentralized data ledger while at the same time enabling an independent freshness evaluation process utilizing AI systems, it is believed that this study will offer improved levels of trust, accountability, and informed decision-making at the consumption end. It is also an intention of this research work to validate its own feasibility in terms of applying the proposed two-layer model.

1.3 Objectives

The primary objective of this research is to design and implement an integrated AI and Blockchain-based system capable of ensuring food safety, detecting food freshness, and preventing counterfeit product circulation. To achieve this, the study focuses on the following specific objectives:

i. Integration of AI and Blockchain for food safety and authentication.
ii. To design different models for training (Random Forest, XGBoost, and LSTM) that have the ability to examine images of food items for the purpose of classifying them as either fresh or expired.
iii. Develop and launch the blockchain-based smart contract on the Ethereum Sepolia test environment to securely store immutable data such as the product ID, name, brand, date of production, date of expiry, and images of the products stored on IPFS and interact with the system via MetaMask-enabled Web3 authentication.
iv. To creating secure SHA-256-based QR codes that link product information with a cryptographic hash for verification by consumers.
v. Blockchain-based security framework that ensures transparency, integrity, and trust through decentralized smart contracts and immutable records.

The above objectives form the basis for the development of a strong, secure, and smart system for improving the safety and authentication of food.

1.4 Methodology

The methodology used in this research work is a structured multi-stage process that integrates Artificial Intelligence, Blockchain, decentralized storage solutions, and Web3 technologies to develop an end-to-end food safety and authentication solution. The process involves dataset preparation, model development, smart contract development, and verification testing stages. We used RF, XGB and LSTM for model training and food freshness detection. Consumer can scan food images and check the freshness using this. Then we developed smart contract using Remix IDE. We used IPFS for data storage by using the Pinata API. We used Metamask as the wallet service. The sellers put the required information about the item into the blockchain and then create a QR code that can be verified; the QR code is stored in the IPFS. Consumers can verify the items by scanning the images of the QR codes.

1.5 Research Outcome

For this research, IPFS was used for the storage of the data through the Pinata API, and MetaMask served as the cryptocurrency wallet. The main objective was to develop a comprehensive system by integrating the prediction of the freshness of food using artificial intelligence, coupled with a system for authenticating a product using a blockchain. The system was fully developed, tested, and validated using real-world datasets, machine learning experimentation, IPFS for storing the data, and a fully functional smart contract on the Sepolia test environment on the Ethereum platform. The main research findings can be highlighted by the following summaries:

i. Performance and Validation of AI-Based Freshness Detection

The experiment shows that it is possible to classify food freshness using images through machine learning. Three models were developed:

- **Random Forest**
- **XGBoost**
- **LSTM-based deep learning model**

Preliminary tests revealed that while the Random Forest and XGBoost models were functioning reasonably well, they were limited by issues of imbalance in their respective data samples and noise in their data. The inclusion of the Long Short-Term Memory (LSTM) model, designed to identify the spatial and temporal characteristics of the images, has proved to increase accuracy considerably. The results validate that the use of Deep Learning models like the proposed LSTM model is robust and can be employed for the assessment of food quality, specifically in the context of spatial and temporal characteristics of the images related to food quality and the spoilage process.

ii. Effectiveness of the Multi-Model AI Framework

The use of the three models enabled a comparison analysis through empirical testing, as shown below:

- Random Forest, LSTM, and XGBoost models predict the freshness of foods, while voting within the three models gives the final prediction.
- The combined process of the three models will improve the accuracy of predictions and limit errors of misclassification for various types of foods.

In general, the AI part is a very effective and speedy approach for the automatic freshness classification.

iii. Successful Deployment of a Blockchain-Based Product Authentication System

One of the core results obtained from this work is related to the development of an authentication system for a product that is resistant to tampering using a smart contract that on the Ethereum Sepolia test network. The blockchain-based system was able to:

- This component details the on-chain storage of product information, such as the product number and name, brand name, and product images stored on IPFS.
- It also includes a SHA-256 QR code link function for a tamper-proof connection between the product and its data on the blockchain.
- Web3 authentication by MetaMask is used to allow only authorized sellers to enter data into the product database on the blockchain.
- Also used is IPFS decentralized cloud storage for tamper-proof product images and access to such images at all times.

All these components show how blockchain offers such capabilities as immutability and security to counteract the leading trend of counterfeits of packaged products.

iv. Enhanced Transparency, Traceability, and User-Level Trust

A integrated architecture that incorporates components from AI and Blockchain systems will enable end-consumer level traceability and interpretability:

- Customers are able to scan a QR code in order to immediately view validated product information on the blockchain.

- It detects anomalies in the scanned QR hashes as well as any related storage information.
- This freshness module based on AI works independently and provides an added safety component by judging food quality irrespective of seller assertions.

When combined, these factors set the basis for a two-step verification process that boosts trust between the company and the consumer, while also reducing the possibility of illicit transactions and increasing the clarity of the supply chain process.

1.6 Organization of the Report

The report consists of six chapters, structured in the following way:

i. **Chapter 1 - Introduction:** This chapter begins the research by introducing the subject of issues related to food safety. Additionally, it establishes the goals and objectives of the research.
ii. **Chapter 2 - Background:** It involves the analysis of the theory underlying the research, a review of the relevant literature, and a gap analysis.
iii. **Chapter 3 - Research Methodology:** This gives a description of methodology, system design, project planning, and task allocation.
iv. **Chapter 4 - Implementation and Results:** This chapter will describe the environment settings and the performance achieved by the system.
v. **Chapter 5 - Engineering Standards and Design Challenges:** The current chapter will discuss the issue of standards in engineering and the influence of societal and environmental factors and challenges in designing solutions to the problems associated with such standards.
vi. **Chapter 6 - Conclusion & Future Work:** he concluding chapter provides a summary of the results and possible ways for future improvements.

Chapter 2

Background

In this chapter, an in-depth review has been conducted to point out the current knowledge available in the existing body of literature on food quality evaluation systems utilizing AI and food authentication systems that make use of blockchain. The theoretical basis of computer vision-based food freshness assessment has been described here. Also, the current state of research on food supply chain transparency and the shortcomings of existing food safety solutions have been identified.

2.1 Introduction

Food safety has become a key area for strategic concern as global supply chains expand and increasingly become more complex and connected through technology. The traditional kind of 'reaction-based control' is increasingly being substituted by a 'predictive, data-driven approach' that has the potential to 'detect spoilage, contaminants, and fraud' before the point of reaching the consumer. The kind of change that is taking place has been adequately defined by the authors et al., and as they state, 'convolutional neural networks, hyperspectral imaging, and blockchain traceability systems allow early-stage pathogen detection and quality monitoring, but the accuracy achieved has been found to come from carefully selected images, reducing the set's ability to generalize [1]. Simultaneously, blockchain technology has been pioneered as a decentralized ledger system that safeguards each and every food chain transaction through immutability and transparency [3]. The role of a decentralized ledger system in overcoming information asymmetry in perishable food product surveillance has been explained by Duan et al., and the systematic review by Hema & Manickavasagan involving 80 studies has authenticated that blockchain enhances recallability and speeds up the recall process along with instilling confidence in the consumer at the expense of a significantly high barrier to implementation [4]. Ellahi et al. further mention under-exploited drivers like food donation, supply chain financing, and waste management, which call for more comprehensive data integration [5]. These above-mentioned challenges can be overcome by the use of private blockchain solutions like Hyperledger Fabric as proposed by Oh et al., which makes it possible to "immutably record the real-time data provided by the IoT sensors" [8]. However, the quality and availability of the incoming data present a significant limitation to the present capabilities of the current state of the art of AI; Dimitrakopoulou and Garre state that "if comprehensive and unbiased data isn't fed into AI models, these won't be able to make meaningful and transparent decisions" [6]. In the wake of the above-discussed findings, there is an apparent need to work towards a research plan that promotes a freshness detection tool based on proper AI solutions in combination with a permissioned blockchain that checks every product number so as to enable "a transparent and trustworthy food safety scheme."

2.2 Literature Review

The landscape of food safety is shifting away from traditional reactive modes of regulations to proactive methods. The work of Balta et al. illustrates this shift, as it shows the use of convolutional neural networks, hyperspectral imaging, and traceability systems based on blockchain to promote early pathogen detection. However, it warns about the accuracy values normally obtained from carefully curated image sets [1]. Zhou et al. provide a systemic view of AI, big data, and blockchain, pointing out that AI obtains freshness signals from heterogeneous sensors, and blockchain guarantees the origin of data from collection, storage, and transfer [2].

The strength of Blockchain technology lies in its immutable, transparent ledger, creating an equalizer of information. Duan et al. demonstrated the complement of a decentralized ledger and a smart contract to close the traceability problem in a perishable food chain [3]. The combination of eight decades' worth of research synthesized by Hema and Manickavasagan shows the positive impact of blockchain technology regarding traceability, recallability, and consumer trust, while the cost of implementation and governance issues are still hindering its use [4]. Underused drivers such as food donations, funding, and waste management, among others, are suggested to be better incorporated by combining multimodal data to fully harness the potential of blockchain, according to Ellahi et al. [5].

The quality of the data has a critical impact on the performance of the model. According to Dimitrakopoulou and Garre, the "intelligence" of AI systems is dependent on the availability of good, unbiased data. Data that does not appear comprehensive may later make a seemingly accurate model potentially unreliable [6]. Aslam et al. further elaborate upon this by pointing out that the integration of inspection by AI, predictive analysis, and IoT can revolutionise compliance, but instead is challenged by data privacy and a slow industry rate of adoption [7].

Private ledger technologies solve the privacy and scalability problems facing public blockchain technologies. A system proposed by Oh et al. uses Hyperledger Fabric to fixedly integrate IoT sensor IoT data within a permissioned blockchain, offering a high throughput with no integrity violations, ensuring edge deployment of freshness detectors [8].

Patel et al. demonstrate the relevance of blockchain technology to livestock product supply chains, stressing tampering-resistant traceability, automated execution of smart contracts, and the need for regulatory harmonization to achieve tangible benefits [9]. Based on these results, Kamilaris et al. demonstrate that while there is significant potential for the usage of blockchain technology to greatly promote transparency, traceability, and trust within agricultural and food chains, the lack of scalability and a preponderance of pilot projects instead of operational systems currently limit the effectiveness of widespread usage of this technology within these chains [10].

Taken together, these works underscore that AI-assisted freshness detection, if coupled within a permissioned blockchain for product verification, can provide accurate, interpretable, and scalable solutions for food safety, thus tackling the problems of data, cost, and governance as remarked in the literature.

Table 2.1: Summary of Literature Reviewed.

Author(s)	Year	Title	Methodology	Key Findings
Balta et al. [1]	2025	Food safety - the transition to artificial intelligence systems	Critical literature review together with a SWOT analysis of the strengths and weaknesses of artificial intelligence	AI tools like CNNs, hyperspectral imaging, and blockchain is employed to promote the early indication of food-safety issues but face the lack of transparency, high costs, and a lack of data.
Zhou et al. [2]	2021	Artificial intelligence, big data, and blockchain in food safety	Systemic literature review organized by data-life-cycle stages (collection, storage, analysis, visualization, security).	Synergistic technologies improve surveillance abilities but require large amounts of labeled data and powerful computational resources; blockchain technology ensures data security.
K. Duan, H. Onyeaka & G. Pang [3]	2024	Pioneering food safety: Blockchain's integration in supply chain surveillance.	Literature review of challenges and strategic proposals	The review argues that blockchain technology promotes traceability and thereby facilitates quick responses to food-related outbreaks
V. S. Hema & A. Manickavasaga [4]	2024	Blockchain implementation for food safety in supply chain: A review.	Systematic review with 80 studies (31 conceptual, 10 implementation, 39 case studies)	This review argues that the use of a decentralized ledger allows for real-time and immutable traceability, which leads to the promotion of safety, quality, and sustainability.
R. M. Ellahi, L. C. Wood & A. E-D Bekhit [5]	2024	Blockchain-Driven Food Supply Chains: A Systematic Review for Unexplored Opportunities	Systematic review on 60 frameworks using NVivo text analysis	Transparency, traceability, security are well presented, with contexts as donation, financing, animal-welfare, waste-management being relatively rare
Dimitrakopoulou & Garre [6]	2025	AI's Intelligence for Improving Food Safety: Only as Strong as the Data that Feeds It	An organized cycle of implementation in five steps (sensing, reasoning, and actuating) is analyzed over 29 pages	AI shows its applications in outbreak identification, fraud tracking, and shelf-life estimation, though its precision gets affected by imbalanced data.

Aslam et al. [7]	2024	AI-driven food safety: transforming food inspection, traceability, and compliance in food industry and regulatory bodies: A mini review	Mini-review of current trends in AI tools (ML, computer vision, NLP) along with their integration with IoT.	Current evidence suggests that AI is capable of over 50% reduction in the processing time of documents, apart from improving real-time monitoring.
Oh et al. [8]	2025	Food Safety Distribution Systems Using Private Blockchain	Incorporate the use of IoT sensors and GS1 EPCIS are considered, system performance being tested using the Hyperledger Caliper tool	Hyperledger Fabric blockchain show its throughput capacity to be around 207 TPS, reaching a maximum of 230 TPS with an average latency of 260 ms, while ensuring the consistency of 115,000 transactions.
A. S. Patel et al. [9]	2023	Blockchain technology in food safety and traceability concern to livestock products	Narrative review of blockchain with IoT integration	Assure tamper-proof and real-time information and can eliminate, or at least reduce, the requirement of authorization from a third party.
Kamilaris et al. [10]	2019	The Rise of Blockchain Technology in Agriculture and Food Supply Chains	A systematic literature review in combination with a survey analysis covering 49 blockchain projects classified on the basis of primary application areas in agriculture and food supply chain management.	The results reveal that blockchain technology enhances transparency, traceability, food safety, and trust in food supply chain management; still, it finds very limited application in practice due to immaturity in technology

These table shows the paper studied to plan our work for AI models food freshness and product authentication using blockchain.

2.3 Gap Analysis

Here put summaries the gaps we have found/observed from the related work study, where we intend to contribute.

Table 2.2: Summary of Research Gaps.

Author(s)	Year	Title	Methodology	Gap Analysis
Balta et al. [1]	2025	Food safety - the transition to artificial intelligence systems	Critical literature review together with a SWOT analysis of the strengths and weaknesses of artificial intelligence	Requires strong data governance, standards, and policy guidelines on adoption.
Zhou et al. [2]	2021	Artificial intelligence, big data, and blockchain in food safety	Systemic literature review organized by data-life-cycle stages (collection, storage, analysis, visualization, security).	There exist certain challenges in labeled data, infrastructure, and generalization in models for AI.
K. Duan, H. Onyeaka & G. Pang [3]	2024	Pioneering food safety: Blockchain's integration in supply chain surveillance.	Literature review of challenges and strategic proposals	Legislative delay, interoperability, low awareness; demand for standardization and incentives by the government
V. S. Hema & A. Manickavasaga [4]	2024	Blockchain implementation for food safety in supply chain: A review.	Systematic review with 80 studies (31 conceptual, 10 implementation, 39 case studies)	Recommendations regarding research needs on untapped drivers and geographical expansion
R. M. Ellahi, L. C. Wood & A. E-D Bekhit [5]	2024	Blockchain-Driven Food Supply Chains: A Systematic Review for Unexplored Opportunities	Systematic review on 60 frameworks using NVivo text analysis	Recommendations regarding research needs on untapped drivers and geographical expansion
Dimitrakopoulou & Garre [6]	2025	AI's Intelligence for Improving Food Safety: Only as Strong as the Data that Feeds It	An organized cycle of implementation in five steps (sensing, reasoning, and actuating) is analyzed over 29 pages	Envisions a need for timely, comprehensive, unbiased data, along with a human-in-the-loop solutions approach.
Aslam et al. [7]	2024	AI-driven food safety: transforming food inspection, traceability, and compliance in food industry and regulatory bodies: A mini review	Mini-review of current trends in AI tools (ML, computer vision, NLP) along with their integration with IoT.	The need for harmonized data protocols, privacy mechanisms, and training.

Oh et al. [8]	2025	Food Safety Distribution Systems Using Private Blockchain	Incorporate the use of IoT sensors and GS1 EPCIS are considered, system performance being tested using the Hyperledger Caliper tool	Scalability to larger network and increased industry acceptance still needs to be addressed.
A. S. Patel et al. [9]	2023	Blockchain technology in food safety and traceability concern to livestock products	Narrative review of blockchain with IoT integration	Legal uncertainty in smart contracts, confidentiality issues, a lack of standards
Kamilaris et al. [10]	2019	The Rise of Blockchain Technology in Agriculture and Food Supply Chains	A systematic literature review in combination with a survey analysis covering 49 blockchain projects classified on the basis of primary application areas in agriculture and food supply chain management.	Current proposals are either piloting or still in the concept stage, with limited implementation in the real world, especially in the developing sector, because of the issues related to scalability, privacy, and awareness regarding integration with AI/IoT-based quality assessment systems.

2.4 Summary

Chapter 2 deals with relevant studies, literature reviews and gap analysis of previous works. These helped us to choose our work based on these literature reviews. We learn previous lacking's and the future scope , so that we can make proper planning for our work. These studies focused on proper AI model training for food freshness detection and Blockchain related product authentication system in supply chain and agriculture sector to make the system more reliable and make it transparent. Previous works or trends lacks transparency or any real world applicable solutions, most of the work was conceptual. This convinced us that how our work will shape and the methods used to solve the real world problems using artificial intelligence and blockchain systems in the context of food safety issues.

Chapter 3

Research Methodology

This chapter discusses the methodological design undertaken for the study, along with the architectural design of the proposed system on the combination of AI and Blockchain technology, focusing on food safety and authenticity. Methodological design outlines the approaches used in a study, while design outlines the architectural details of the proposed system, including the data flow.

This proposed system incorporates a synergistic combination of blockchain and artificial intelligence technologies. Machine learning algorithms would be utilized for image analysis of the food items to classify them as fresh and rotten through a user interface. At the same time, the blockchain technology would ensure the secure storage of the product data and image hashes to prevent adulteration. QR codes are produced for the product in order to facilitate customers in checking its authenticity through the blockchain system. Smart contracts ensure the transparency of information storage throughout the supply chain. The proposed system improves food safety, prevents fraud, and boosts consumer confidence with its features for real-time verification and freshness analysis through artificial intelligence.

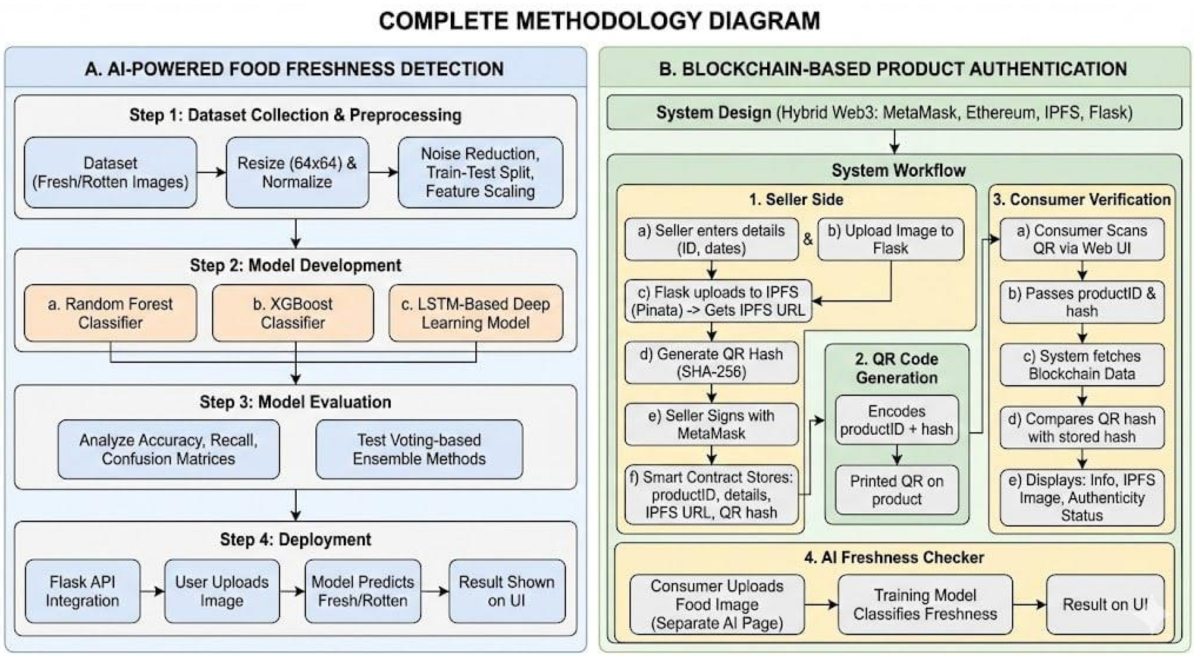


Figure 3.1: Proposed Methodology of AI Powered Food Freshness Detection With Blockchain Based Product Authentication.

Our work is divided into two sections. Which are:

i. Section A : AI Powered Food Freshness Detection
ii. Section B: Blockchain Based Product Authentication

Commonly used notations

Table 3.1: Summary of Notations.

Symbol/Notation	**Description**
I	Input food image
X	Extracted feature vector from an image
Xstd	Feature vector after standardization
y	True class label
y^	Predicted class label
f(x)	Prediction from the decision tree
Fi(x)	Boosted prediction at iteration i
hi(x)	Weak learner at iteration i
η	Learning rate used in XGBoost
ht	Hidden state of the LSTM at time step t
μ	Mean of feature values
σ	Standard deviation of feature values
UID	Unique product identifier
P	Product information set
LIPFS	IPFS link of the stored product image
H	SHA-256 hash value
QR	QR code containing product data
SC	Ethereum smart contract

3.1 AI-Powered Food Freshness Detection

In this stage, a food images dataset is first collected and undergoes rigorous preprocessing procedures like resizing, normalization, as well as removal of noise in order to have uniform data quality. For more accurate detection the images feature such as color, texture was extracted. Then several AI models, namely Random Forest, XGBoost, as well as Long Short-Term Memory networks, are then trained in order to extract patterns associated with freshness. Each model separately judges how fresh a given piece of food is, predicting whether it is either fresh or rotten. The decision is combined into a more reliable one with a voting mechanism based on ensembling machine learning methods. If two or more , means majority output between those three model will indicate the freshness result of that food image. The model of choice can then be applied with a Flask API and used to display results of image freshness on its user interface. User have to enter food images using the API and the result will be shown on the screen.

.

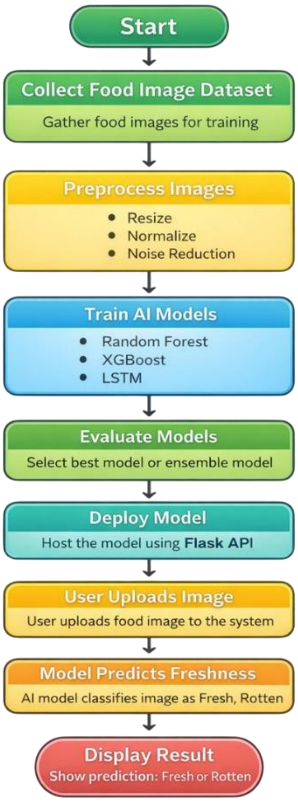


Figure 3.2: Flow Chart of AI Powered Food Freshness Detection.

- ## Algorithm 1

Input: Food images (.jpg, .jpeg, .png, .bmp)
Output: Food freshness results
Step 1: A food dataset consist of 27845 images were collected where each image is manually labeled into two classes:

$$\boldsymbol{Y} \in \{\boldsymbol{Fresh}, \boldsymbol{Rotten}\}$$

Step 2: The dataset is structured into class-wise directories:

- /Fresh
- /Rotten

Step 3: Each image $\boldsymbol{I}$ undergoes preprocessing to reduce variations and improve learning efficiency.

Step 4: All images are resized to a fixed resolution of 64 × 64 pixels:

$$\boldsymbol{I_{resized}} \in \mathbb{R}^{\boldsymbol{64\times64\times3}}$$

Step 5: Pixel values are normalized to the range $\mathbf{0, 1}$ using:

$$\boldsymbol{I_{norm}} = \frac{\boldsymbol{I_{pixel}}}{\mathbf{255}}$$

Step 6: Statistical feature extraction inherently reduces pixel-level noise by summarizing global image characteristics.

Step 7: From each processed image, discriminative features are extracted, including: Color statistics, texture features, flattened pixel intensity vectors.
The extracted feature vector is represented as:

$$\boldsymbol{X} = [\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n]$$

Step 8: Feature scaling is applied using Standardization:

$$\boldsymbol{X}_{scaled} = \frac{\boldsymbol{X} - \boldsymbol{\mu}}{\boldsymbol{\sigma}}$$

Step 9: Split the dataset D into training set Dtrain and test set Dtest:

$$\boldsymbol{D}_{\text{train}} = \{(\boldsymbol{X}_i, \boldsymbol{y}_i)\}_{i=1}^{n_1}, \; \boldsymbol{D}_{\text{test}} = \{(\boldsymbol{X}_i, \boldsymbol{y}_i)\}_{i=n_1+1}^{n};$$
$$\text{where } \boldsymbol{n}_1 = \mathbf{0.8}\boldsymbol{n}, \boldsymbol{n} - \boldsymbol{n}_1 = \mathbf{0.2}\boldsymbol{n}$$

Step 10: Model training:

i. Random Forest Classifier:
An ensemble of decision trees is trained:

$$\hat{\boldsymbol{y}}_{RF} = \text{mode}\{\boldsymbol{T}_1(\boldsymbol{x}), \boldsymbol{T}_2(\boldsymbol{x}), \ldots, \boldsymbol{T}_n(\boldsymbol{x})\}$$

ii. XGBoost Classifier:
Gradient-boosted decision trees are trained sequentially:

$$\boldsymbol{F}_t(\boldsymbol{x}) = \boldsymbol{F}_{t-1}(\boldsymbol{x}) + \boldsymbol{\eta}\boldsymbol{h}_t(\boldsymbol{x})$$

iii. LSTM-Based Deep Learning Model:
The extracted feature sequence is fed into an LSTM network:

$$\boldsymbol{h}_t = LSTM(\boldsymbol{x}_t, \boldsymbol{h}_{t-1})$$

Step 11: Model parameters such as: Number of trees, Learning rate, Number of LSTM units.

Step 12: Each trained model is evaluated using: Accuracy, Precision, Recall, Confusion Matrix.

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP} + \boldsymbol{TN}}{\boldsymbol{TP} + \boldsymbol{TN} + \boldsymbol{FP} + \boldsymbol{FN}}$$

Step 13: A majority voting strategy is applied:

$$\hat{\boldsymbol{y}}_{final} = \text{mode}(\hat{\boldsymbol{y}}_{RF}, \hat{\boldsymbol{y}}_{XGB}, \hat{\boldsymbol{y}}_{LSTM})$$

If at least two models agree, that class is selected as the final prediction.

Step 14: Deploy the selected model using a Flask API.

Step 15: User upload food images via the user interface.

Step 16: The input image will be preprocessed, then inputted to the deployed model.

Step 17: Predict the food freshness category (Fresh or Rotten).

Step 18: Display the results of your predictions in the UI.

Algorithm 1 illustrates the complete process of food freshness evaluation using machine learning and deep learning techniques. In Step 1, the labeled images dataset consist of 27845 images were processed, which consist of classes labeled as "Fresh" and "Rotten." Step 2 classifies the images according to their labeled categories into separate directories. Steps 3 through 8 discuss the image processing steps, which consist of image resizing into 64 × 64 pixels images, followed by normalization, feature extraction and scaling. Step 9 defines the split process of the images into testing and training sets where 20% images (5,569) were used for testing and 80% images (22,276) were used for training. Step 10 and 11 relate to the process of training different algorithms such as the Random Forest Classifier, the XGBoost Classifier, and the Long Short-Term Memory deep learning approach. Step 12 is related to the assessment of the trained models based on metrics like accuracy, precision, and recall values, and also based on the use of confusion matrices. Steps 13 detail the method to obtain the superlearner ensemble result, in which the freshness label is decided jointly if at least two member algorithms agrees. In Step 14, based on the chosen algorithm, the overall final result is produced through a Flask API web service. Steps 15 to 18 deal with human interfaces, whereby pre-processed images are processed by the trained algorithm and the freshness result is communicated to the user as either Fresh or Rotten through extremely graphical interfaces.

3.1.1 Dataset Collection and Preprocessing

A carefully selected and compiled data set with a total of 27,845 images was created and classified into two main categories: Fresh and Rotten. Image resolution was consistently normalized to a standard size of 64×64 pixels. In addition, a preprocessing technique was employed with the purpose of reducing distortions and lighting in the background. Various feature extraction techniques proved effective in extracting critical features concerning texture, color, and deterioration. The preprocessed data set was divided equally into a testing and a training set. Feature scaling was done appropriately.

3.1.2 Model Development

There are three different models that were considered to evaluate the freshness of the food by analyzing the image information. The Random Forest Classifier algorithm was considered for its interpretability and ability to deal with the decision boundaries that are non-linear. The XGBoost Classifier algorithm was considered because of its gradient boosting technique. A long short-term memory (LSTM) deep learning approach was proposed to incorporate the sequential and spatial patterns present in the features of the images. It enables the learning of the temporal dependencies of the features, which could improve the performance of the classifier. The use of various models helped to provide a comprehensive analysis to result in a more accurate prediction using the ensemble method.

3.1.3 Model Evaluation

To judge how each of these models fared, we examined their accuracy, recall, confusion matrix, and classification reports. These provided a very clear idea of how well each of them predicted, as well as where errors were occurring. We used confusion matrices, in particular, to identify where errors were being made, in terms of false predictions of both fresh and rotten food. In order to make predictions more reliable, a voting-based ensemble strategy was used for the Random Forest, XGBoost, and LSTM models. Each of the models made a separate prediction for a particular picture using the strategy. If at least two models agreed on the same output, the output class was selected as the final answer.

3.1.4 Deployment

The trained models and the ensemble strategy were incorporated into a Flask API. The output of the models was serialized and loaded efficiently for quick responses during inference. Users can submit a picture of a dish through a web interface. The picture will go through the same preprocessing step that was done during training. Relevant features are picked from the image, and they are then sent to the deployed models for prediction. Based on the result of the voting technique, an image is labeled as either Fresh or Rotten. The prediction is then displayed on a graphical user interface with appropriate visual feedback.

3.2 Blockchain Based Product Authentication

In this phase, the seller proves their authenticity with MetaMask, while product details are established on the blockchain. Seller can enter product ID, name, brand, dates. The image associated with the product is then uploaded to IPFS, with an SHA-256 hash generated for its integrity. A QR code is made which will be stored on IPFS using the product details and printed on the product, and the product number and hash are embedded in it. The code is scanned using an app to call up the blockchain information, and the hash is checked to determine if the product is genuine.

.

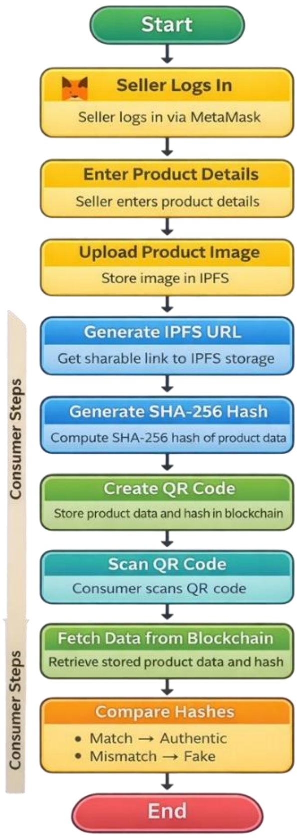


Figure 3.3: Flow Chart of Blockchain Based Product Authentication.

- ## Algorithm 2

Input : QR generation by entering product details.
Output : Fetching product information from QR images.

Step 1: The seller starts the registration process by verifying himself/herself through MetaMask.

Step 2: The Ethereum address of the seller is confirmed to ensure its genuineness.

Step 3: The seller begins entering product information. Let '$\boldsymbol{P}$' represent the product object:

$$\boldsymbol{P} = \{\text{Product Name, Brand, Manufactured Date, Expiry Date, Product Image}\}$$

Step 4: The product image is uploaded by the seller through the Flask backend.

Step 5: The product image is uploaded into IPFS storage using Pinata.

Step 6: An IPFS URL specific to the uploaded image is created.

Step 7: Generate the SHA-256 hash based upon the Product ID and the IPFS URL.

Step 8: The Product ID along with the generated hash should be encoded in a QR Code.

$$\boldsymbol{QR_P} = \text{Encode}(\boldsymbol{ID_P}, \boldsymbol{H_P})$$

Step 9: Executing the Ethereum Smart Contract to store the following: Product ID, Product Information, IPFS URL, QR hash.

$$\boldsymbol{SC} \leftarrow \{\boldsymbol{ID_P}, \boldsymbol{P}, \boldsymbol{URL_{IPFS}}, \boldsymbol{H_P}\}$$

Step 10: The seller signs the blockchain transaction through MetaMask.

Step 11: The consumer begins a scan of a QR code using the web-based user interface.

Step 12: Product ID and hash are obtained from the QR code scan.

$$\boldsymbol{ID_P}, \boldsymbol{H_P} \leftarrow \text{Decode}(\boldsymbol{QR_P})$$

Step 13: The product data stored in the blockchain are retrieved.

Step 14: The hash value extracted from the QR code is matched with the hash value recorded on the blockchain.

Step 15: If both hashes are equal, mark the item as Authentic.

Step 16: If a mismatch is found, mark it as either Tampered or Fake.

Step 17: Offer product information, the IPFS image, and authenticity status to the consumer.

Algorithm 2 describes a secure blockchain network solution for authenticating products to counter and maintain consumers' trust. In Steps 1 and 2, the vendor authenticates a product on MetaMask by providing a correct Ethereum address. In Step 3, the vendor enters essential product details such as product name, brands, date of manufacture, date of expiration, and a photo of the food. In Steps 5 and 7, a photo of the product is uploaded on the Flask server and an IPFS link is generated. In Step 8, a SHA-256 hash is generated using the Product ID and IPFS URL, which is encoded into a QR code. In Step 9, an Ethereum smart contract function is executed and then signed using MetaMask to get the Product ID, product info, IPFS URL, and QR hash permanently etched on the blockchain. In Steps 11-13, the buyer scans the QR code using a web interface, which then resembles the extraction of the Product ID and hash value, fetching the data materializing on the blockchain, and finally authenticating the product using a comparison between the two hash values. Finally, in Steps 14-17, on successful matching between the two hash values, the product gets authenticated; else, they identify the product to be tampered with, finally displaying the authenticated product info, IPFS pic, and authentication status.

3.2.1 Seller Side

The seller records details about the product: its code, name, trademark, manufacturing date, and expiration date. The image of the product is then uploaded to the Flask app. The Flask app transfers this image to IPFS through Pinata and then sends back an IPFS URL. The hash value of the QR code is produced using the SHA-256 hashing algorithm. The seller confirms and signs the transaction via MetaMask. The smart contract holds data pertaining to transactions: productID, name, brand, prodDate / expDate, IPFS image URL, QR hash.

3.2.2 QR Code Generation

Both the product code and its associated hash value are encoded in the QR code. The QR code can be attached to or printed on the product for instant verification. QR code image can be scanned or shared using link by seller. The QR image is stored in Pinata IPFS.

3.2.3 Consumer Verification

The consumer uses the web interface to scan the QR code.The QR code passes the values of productId and hash as arguments automatically. The system accesses data stored within a blockchain. The hash obtained from the QR code is compared to the stored hash value. The result of verification is shown: product information, IPFS image, authenticity status.

3.3 Proposed Methodology/ System Design

The proposed framework design consists of two modules. The two modules will enable the integration of AI analysis for evaluating the freshness of the food and the usage of blockchain methods for authenticating the involved food item.

Within the freshness analysis using the AI-related task, the respective workflow strictly follows the traditional machine learning approach, which entails image processing, feature selection, model training, model evaluation, as well as prediction within the following models: Random Forest, XGBoost, as well as the Long Short-Term Memory model. Besides, majority voting is incorporated to improve the prediction accuracy of the respective model and detect real time food freshness using images input given by the consumer.

The blockchain authentication module focuses on secure product registration and verification using Ethereum smart contracts, MetaMask, IPFS, and QR codes. The hash value of the products, alongside the product information, is immutable and recorded on the blockchain. The product images are decentralized and stored in IPFS. The link between the product and the information on the blockchain is made using the QR code.

In conclusion, the design of the system allows for the correct determination of product freshness using artificial intelligence, as well as secure authentication using blockchain.

3.4 Detailed Methodology and Design

This section describes the overall methodological framework adopted in the project. It presents the alternative solutions provisionally considered and their feasibility analysis, and then explains the rationale behind the eventual choice made on the two-tier system involving the integration of AI food freshness and blockchain product authentication. The system consists of self-contained and mutually supportive components that combined cover the fundamental research question concerning food safety and the verification of unadulterated products.

3.4.1 Overview of Methodological Approach

The approach includes two parallel technology streams:

i. **AI Pipeline**, a system used to measure the freshness level of food products based on images.
ii. **Blockchain Pipeline**, which provides an immutable onchain product authentication process through QR code, smart contracts, and IPFS.

Such pipelines work independently but together provide the complete food safety solution. The research follows the standard methodology flow:
Problem Identification → Data Collection → Model Building → System Integration → Evaluation → Reporting

3.4.2 Initial Solution Considerations

Before finalizing the system, multiple approaches were examined:

A. **Centralized Database System**

Pros:
- Easy to implement
- Quick support for creation, read, update, and delete operations
- Low-cost infrastructure

Cons:
- Vulnerable to tampering
- Central point of failure
- Not suitable for anti-counterfeit use cases

Reason for rejection:
Exporters Consumer trust and security come first. It is impossible to guarantee data integrity and transparency in a centralized structure.

B. **Manual Inspection + QR Code Labels**

Pros:
- Low technical complexity
- Enables easy industry adoption

Cons:
- QR codes alone can be forged
- The manual inspection tasks are time-consuming and subject to variability
- Lack of scientific basis for freshness of food

Reason for rejection:
The method fails to address the issue of product authenticity or scientific food assessment.

C. **Traditional ML Models (SVM, Logistic Regression) for Freshness Detection**

Pros:
- Should require fewer computational resources
- Easy to train

Cons:
- Suboptimal performance on image data
- Lack of Ability to Extract Deep Visual Features
- Limited real-world accuracy Rationale

Reason for rejection:
The dataset contains real-world fruits, vegetables, and meat, all of which have complex textures and cannot be computed through traditional machine learning algorithms.

3.4.3 Final Selected Solution

On the basis of feasibility, security, accuracy, and contribution towards research, the proposed methodology has been selected as below:

A. **AI-Based Freshness Detection**

Why This Solution Was Selected

✓ Works without human intervention
✓ Supports real-time image classification
✓ Provides quantitative indicators (Fresh/Rotten + Confidence %)
✓ Useful for both consumers and sellers

Design Choices
- Decision-making through the use of Random Forest, Long Short-Term Memory (LSTM), and XGBoost
- Use of a Voting Ensemble for increased reliability

Advantages
- Attains high accuracy (over 80% after fine-tuning)
- Is resistant to lighting variations and noise
- Functioning entirely offline after the training phase has been completed

B. **Blockchain-Based Product Authentication**

Why Blockchain?

✓ Immutability prevents modifying product information

✓ Public availability increases consumer trust

✓ Smart contract ensures verifiable proof of origin

✓ Eliminates counterfeit products in supply chain

Design Choices

- Ethereum Sepolia test network
- Solidity Smart Contract
- MetaMask Wallet Signatures
- Image storage on IPFS (Pinata)
- QR codes containing hashed product information

Advantages

- Risk of tampering eliminated
- Decentralized verification
- Write permissions restricted to sellers; read-only access for buyers
- Increased transparency & traceability

C. **Independent Dual-Layer System Design**

Both modules operate independently but serve different roles:

AI Freshness Detection : Verifies physical condition of food.
Blockchain Verification : Verifies authenticity & product details.

This design ensures:

- The blockchain system works even if the AI module fails (for example, in the case of poor image quality).
- If there are failures in the blockchain subsystem (e.g., network problems), the AI component will keep working.
- The system as a whole retains functionality under varying conditions

3.4.4 System Architecture Summary

A methodological framework has been structured into three hierarchical layers:

i. **Data Processing Layer**

- Preprocessing images of food (resizing, normalization).
- Train/Test Split
- Data Augmentation

ii. **AI Processing Layer**

- Models: Random Forest, XGBoost, Long Short-Term Memory
- Ensemble voting classifier
- Model evaluation metrics: accuracy, recall, confusion matrix

iii. **Blockchain Layer**

- Product registration by the seller.
- IPFS-based storage
- Smart contract write functions

- QR code encoding (SHA-256), along with product information
- Consumer verification

Each module has clearly defined inputs, processing, and outputs.

3.4.5 Rationale Behind Final Methodology

The chosen methodology is applicable to this project on several grounds:

i. Artificial intelligence improves food safety.
ii. The blockchain technology helps overcome the issue of counterfeiting and maintains authenticity.
iii. The QR code has an easy and user-friendly interface that links the technology and the consumer.
iv. Decentralized systems encourage trust, especially in an unreliable supply chain.
v. A modular architecture improves the scalability of the system.
vi. Dual pipeline design provides redundancy.

3.5 Project Plan

This project involved a series of systematic phases, beginning with problem analysis and requirement identification through an appraisal of current food safety and anti counterfeit solutions. This stage was then followed by data gathering and preprocessing, which involved food image labeling, resizing, normalization, and preprocessing for feature extraction. A number of AI solutions were developed, including Random Forest, XGBoost, and Long Short-Term Memory networks (LSTM), and were trained and tested for performance based on standardized quantifiable factors, a voting algorithm being incorporated to boost accuracy. Additionally, a blockchain and smart contract approach was incorporated for a trustworthy and secure food item registration and verification system using Ethereum smart contracts, Meta Mask, IPFS, and QR codes.

3.6 Task Allocation

This table depicts the timeline of the principal activities in each period of the project, from week 12 to week 48.

Tasks	**Weeks**																		
	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
Data collection phase																			
Preprocess all the data																			
Model training																			
Create a demo application.																			

3.7 Summary

This research project makes use of AI techniques in order to determine the freshness of food from images and also incorporates blockchain in order to ensure the accuracy of the product information through registration and the QR code system. The project schedule lasts from Week 12 through Week 48 and involves data collection and blockchain registration and then preprocessing and food images labeling. We then train artificial intelligence algorithms to classify the freshness and test these results for accuracy on the blockchain data. Third, we developed an application for the vendors to input their product data into the blockchain and produce the QR code for it.

Chapter 4

Implementation and Results

This chapter describes the implementation aspects and experimental outcomes of the proposed Methodology. It discusses the development environment used, the performance measures used to gauge the accuracy of the Methodology, and a comprehensive comparative analysis conducted among the proposed Models.

4.1 Environment Setup

The "AI-Powered Food Freshness Detection with Blockchain-Based Product Authentication" system developed in this hybrid environment is capable of handling deep learning tasks as well as blockchain interactions. The system setup considered for this project helps in achieving high-performance computing for image processing tasks and smart contract execution.

4.1.1 AI System Environment

The AI subsystem focuses on food image processing and freshness classification using machine learning and deep learning models. This module operates independently of the blockchain and is responsible for predicting whether a food item is Fresh or Rotten.

AI Tools and Technologies

Table 4.1: Tools for AI related phase.

Category	Tool / Technology	Purpose
Programming Language	Python 3.12	Core language for model training, inference, and integration
Image Processing	OpenCV	Reading, resizing, and preprocessing food images
Machine Learning	Scikit-learn	Training Random Forest classifier
Gradient Boosting	XGBoost	High-performance tree-based classification
Deep Learning	TensorFlow & Keras	Training and deploying LSTM-based freshness model
Model Persistence	Joblib	Saving and loading trained ML models
Data Handling	NumPy	Numerical computation and feature handling
User Interface	Tkinter	Desktop-based interface for AI freshness scanning
Platform	Pycharm	Used for all the coding components

Role of AI Tools

- OpenCV preprocesses food images by resizing and extracting visual features.
- Random Forest and XGBoost provide robust traditional machine learning baselines.
- LSTM captures sequential feature patterns for improved freshness detection.
- Voting ensemble logic combines predictions from RF, XGBoost, and LSTM to improve reliability.
- Tkinter UI allows users to upload images and view freshness results interactively.

4.1.2 Blockchain System Environment

The blockchain subsystem ensures product authenticity, traceability, and tamper resistance. It is used for product registration by sellers and QR-based verification by consumers.

Blockchain Tools and Technologies

Table 4.2: Tools for Blockchain Related Phase.

Category	Tool / Technology	Purpose
Smart Contract Language	Solidity	Writing immutable product registration logic
Blockchain IDE	Remix IDE	Smart contract development and deployment
Blockchain Network	Ethereum Sepolia Testnet	Cost-free testing environment
Wallet	MetaMask	Secure transaction signing by sellers
Blockchain API	Web3.py	Python-based interaction with smart contracts
QR Processing	OpenCV QRCodeDetector	Decoding QR codes from images
Decentralized Storage	Pinata IPFS	Storing product images off-chain
Backend Framework	Flask	Handling image upload and IPFS integration
Networking	HTTP / REST APIs	Communication between frontend, backend, and blockchain
Frontend	HTML & CSS	Web-based seller and consumer interfaces

Role of Blockchain Tools

- Solidity smart contracts securely store product metadata and QR hashes.
- MetaMask ensures that sellers sign transactions without exposing private keys.
- Web3.py retrieves on-chain product data for verification.
- Pinata IPFS provides decentralized and tamper-resistant image storage.
- QR codes link physical products to on-chain records for instant consumer verification.

4.1.3 Hardware Configuration

Table 4.3: Hardware Requirements.

Component	Specification
Processor	Intel Core i5 / i7 or equivalent
RAM	Minimum 8 GB
GPU (optional)	NVIDIA GPU or Google Colab T4 for model training
Storage	SSD recommended for faster data access

The hardware configuration supports efficient image processing, model inference, and blockchain interaction, while remaining suitable for academic and real-world prototyping environments.

Implementational Workflow and Dataseset Collection:

In this workflow, the proposed integrated AI-Blockchain solution can ensure the authenticity and quality verification of the product. The entire process, from data acquisition to model creation and the use of blockchain for traceability, has been described here. In the AI model, the classification of the product image will happen regarding whether the product is fresh or rotten, and the blockchain part will keep the product, seller, and IPFS-linked QR code data securely.

4.2 AI Performance Evaluation

In order to determine the efficiancy of the developed system, we conducted a detailed comparative study among three machine learning techniques: Random Forest, XGBoost, and Long Short-Term Memory. These techniques were tested using standard classification metrics, including Accuracy, Precision, and Recall.

4.2.1 Model Accuracy Comparison

The primary evaluation metric was the model's ability to classify food images into “Fresh” or “Rotten.” It is clear from the comparative chart given below that the Random Forest model performed better than other models in this particular data set.

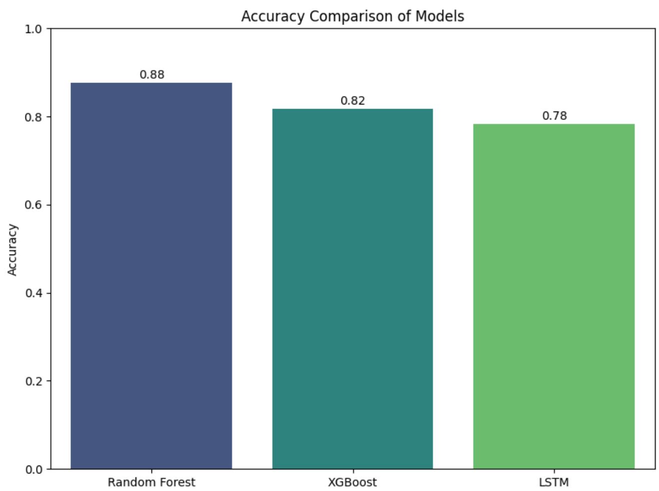


Fig 4.1: Model Accuracy Comparison between RF,XGB and LSTM.

Analysis:

1. **Random Forest:** Random Forest had the highest accuracy of **88%**, meaning that the ensemble method using decision trees successfully utilized the derived feature vectors from the food images.

2. **XGBoost:** Accuracy of **82%** achieved by XGBoost reflects excellent results and a slightly lesser degree of generalization compared to Random Forest.

3. **LSTM:** On accuracy, Long Short-Term Memory (LSTM) networks had an accuracy of **78%**. Though LSTMs work well on sequence data, having a fixed image context made tree-based methods (RF & XGBoost) more effective in identifying feature correlations pertaining to freshness.

4.2.2 Precision and Recall Analysis

To ensure the system minimizes false positives (labeling rotten food as fresh) and false negatives, Precision and Recall metrics were analyzed for Class Fresh and Class Rotten.

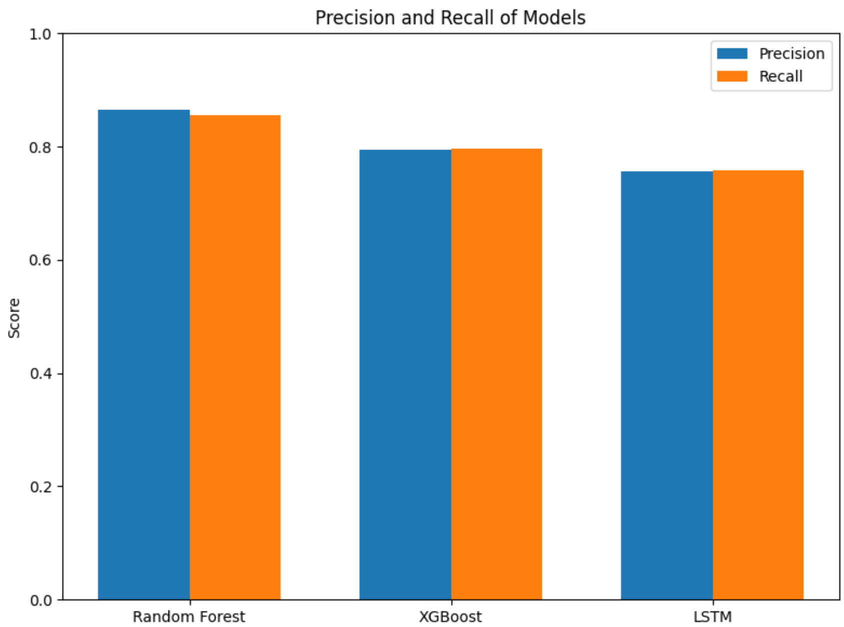


Figure 4.2: RF, XGB and LSTM Precision and Recall metrics.

The chart compares Random Forest, XGBoost, and LSTM on precision and recall. Random Forest performs best (≈0.88 for both), showing strong accuracy and reliability. XGBoost is moderate (≈0.82), while LSTM is lowest (<0.80). Overall, ensemble methods outperform LSTM, and Random Forest is the most suitable choice especially where high recall is critical for food safety. Final freshness result for any food images will be shown based on voting between these three models and its output.

4.2.3 Baseline Model Analysis (Bias Detection)

Confusion matrices were generated to visualize the exact number of correct and incorrect predictions for each model.

- **Random Forest:** The high number of True Positives (2751) and True Negatives (2127) and a small number of False Positives (331) shown by the Random Forest model illustrate its effectiveness for use in a production environment.

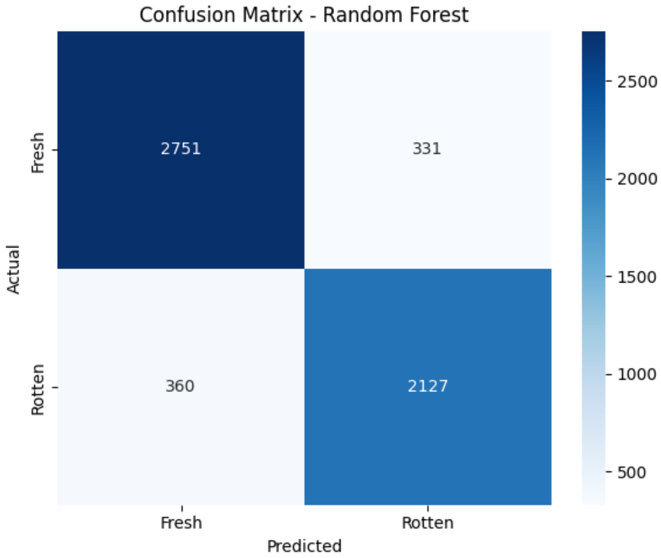


Figure 4.3: Random Forest Confusion Matrix.

- **XGBoost:** The high number of True Positives (2750) and True Negatives (1979) and a slightly greater number of False Positives (512) shown by the XGB model illustrate its effectiveness for use in a production environment.

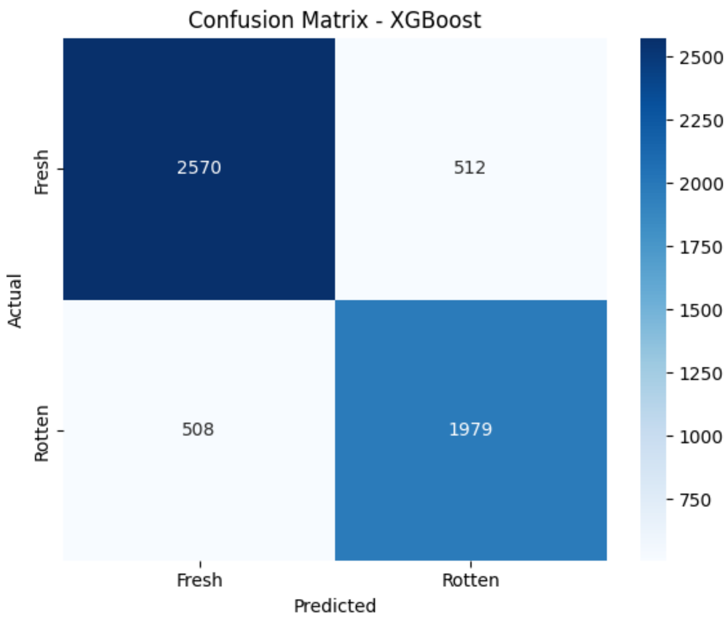


Figure 4.4: XGBoost Confusion Matrix

- **LSTM:** The number of True Positives (2477) and True Negatives (1884) and a small number of False Positives (605) shown by the Random Forest model illustrate its effectiveness for use in a production environment.

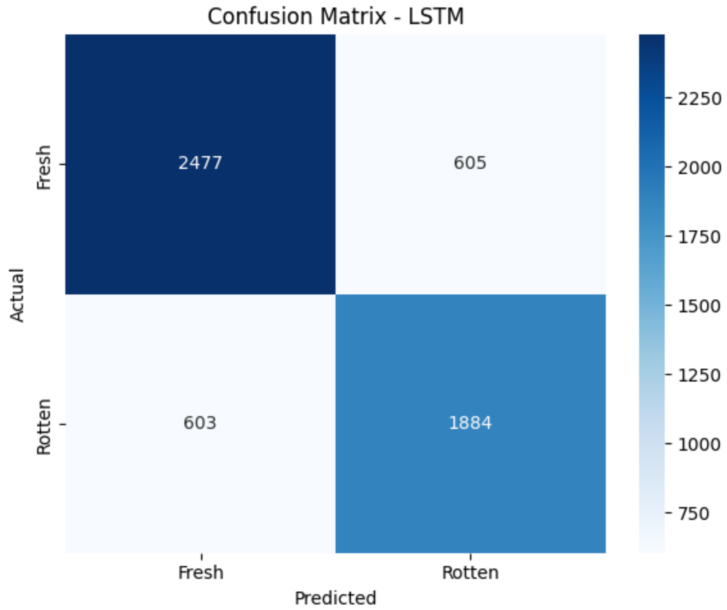
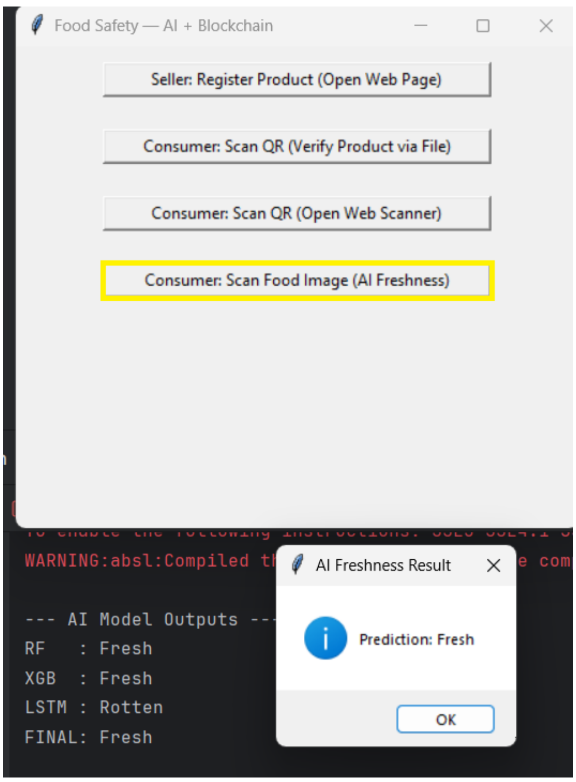


Figure 4.5: LSTM Confusion Matrix.

4.2.4 User Interface:



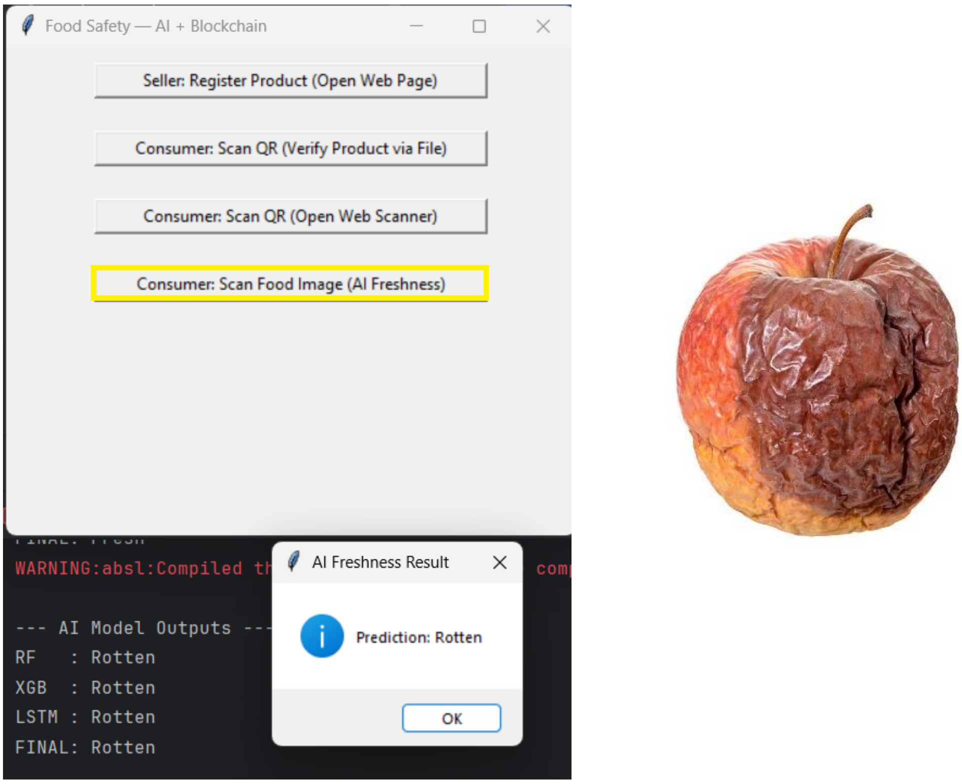


Figure 4.6: The integrated application UI showing the AI Freshness Result.

The UI demonstrates the successful unification of the project objectives: a user can check the physical quality of the food using the system (AI Result) independently. The interface showing both Fresh and Rotten resulted in the system using proper voting methods between the three AI model training.

4.3 Blockchain Perfomance Evaluation

The performance analysis of the blockchain-based system indicates that it provides firm and trustworthy product authentication via the use of Ethereum smart contracts and IPFS. With regards to confirmation times on the Sepolia test net, product registration transaction confirmations take 10 to 30 seconds, which is suitable for a single-time seller configuration, and product authentication by the consumer happens in near real-time via simple read-only contract queries. Additionally, gas prices remain minimal due to small on-chain storages, where large files such as product images are stored off-chain via IPFS. The proposed system provides scalability via the use of a hybrid solution that involves both on-chain and off-chain components, which also provides resistance to tampering and data integrity. Signing via MetaMask provides an added security benefit due to the lack of storage of private keys on the backend server side. Therefore, in light of performance, cost-effectivity, and security considerations, the blockchain-based layer provides an optimum balance in both performance and security in terms of product authentication for real-world food products.

4.3.1 Cost Analysis

In this part, we analyzed how much our suggested system would cost, focusing on the gas costs related to different processes in the smart contract. Based on the currency rate at the selected date and time.

Table 4.4: Gas Cost Analysis.

Function Name	Transaction cost (ETH)	Execution cost (ETH)	Gas uses	In USD ($)
Contract deploy	0.0004	0.0004	1,506,857	1.29
Product Registration	0.0007376475	0.0007	491,765 (1.5 Gwei)	2.26

Cost analysis for the blockchain-based food safety system suggests that the cost of deploying the smart contract integrating Remix IDE with Metamask wallet was 0.0004 ETH, which was associated with the execution cost of around $1.29. However, the cost of the product registration was marginally higher at the rate of 0.0007376475 ETH (execution cost of around $0.0007), which was approximately $2.26. The above results clearly confirm that the cost of deploying the contract is very low as compared to the registration of the products, which requires a larger number of gas units (approximately 1,506,857 at 1.5 Gwei) because of the associated data processing requirements of the contract.

4.3.2 User Interface/Web Interface:

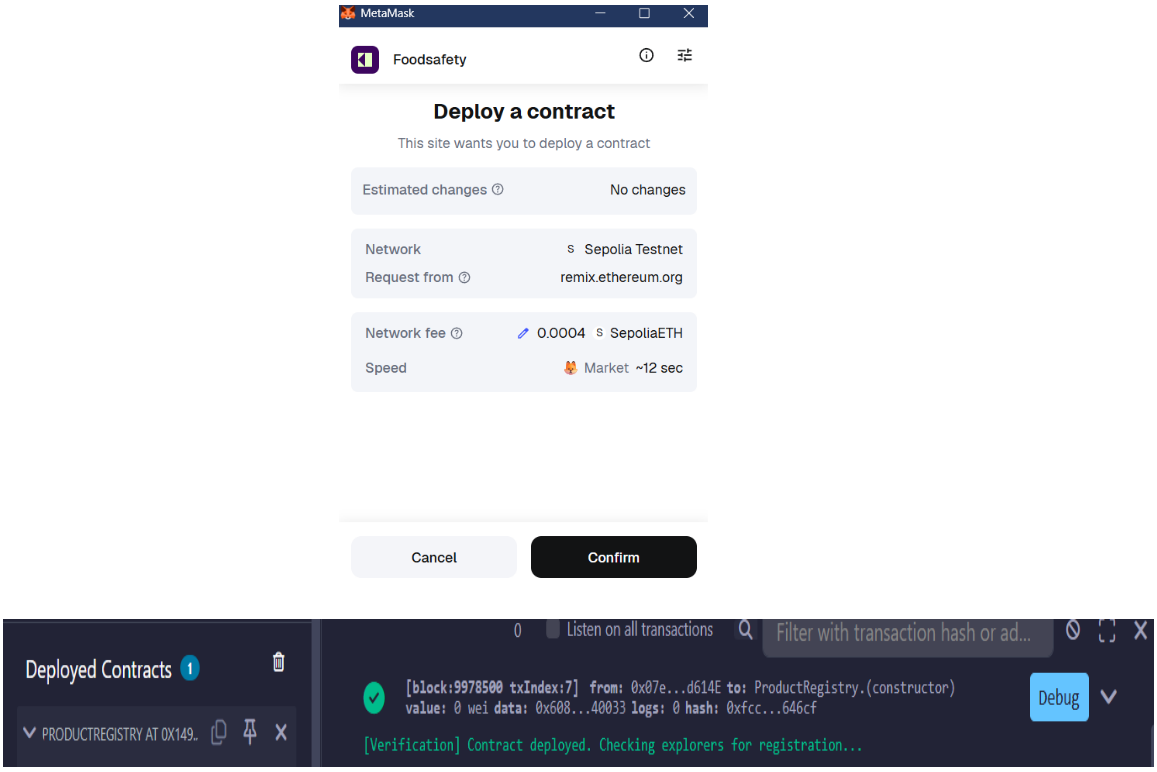


Figure 4.7: Blockchain Smart Contract Deployment Using Metamask.

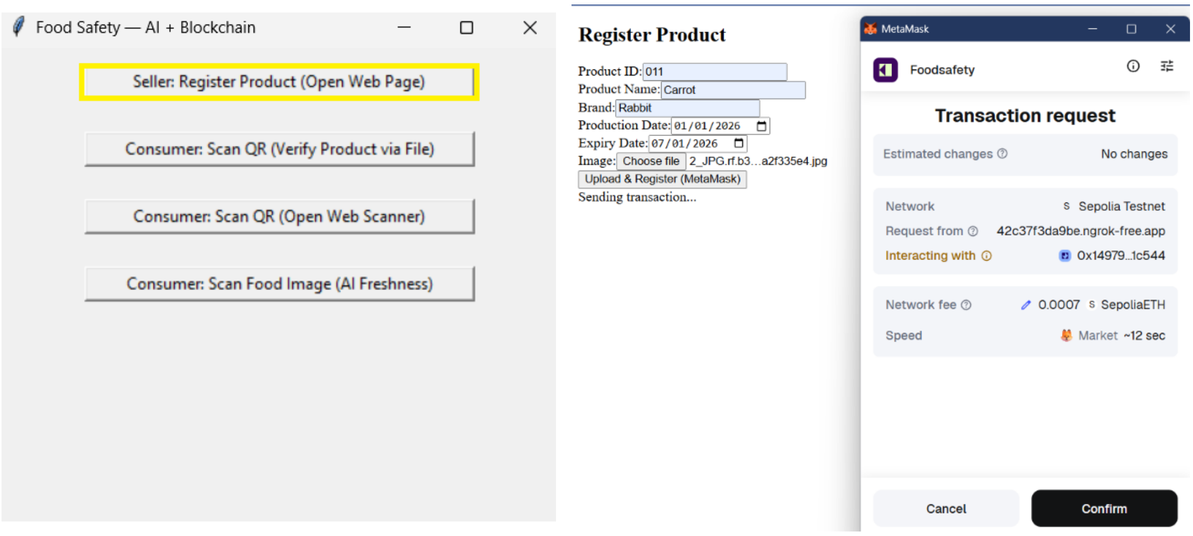


Figure 4.8: Product Registration Using Metamask.

Figure 4.9: QR Generation Encoding Product Information.

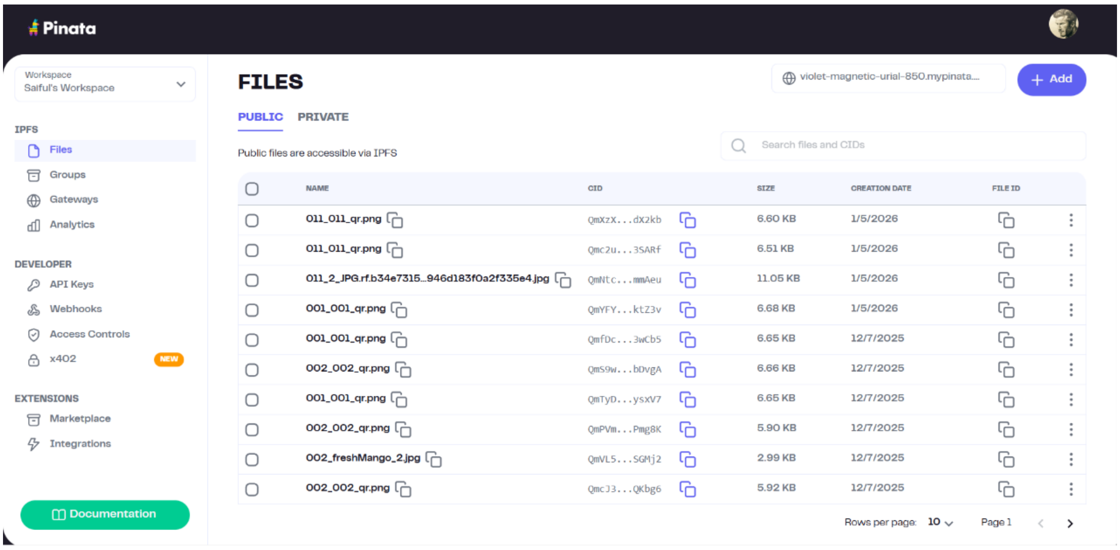


Figure 4.10: Storing Images In Pinata IPFS Storage.

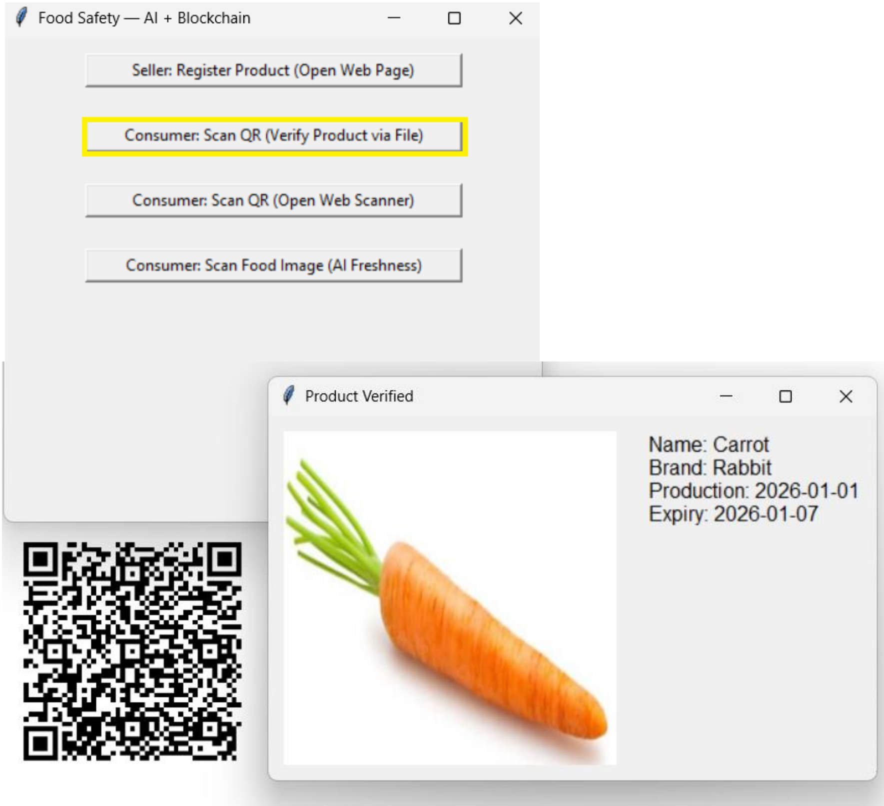


Figure 4.11: Decoding Product Details By Scanning QR Image.

The UI demonstrates the successful unification of the project objectives: seller can register product information on blockchain and user can independently verify its digital identity (Blockchain Scan) in a single workflow.

4.4 Comparative Analysis

4.4.1 AI Models for Food Freshness Detection

Model accuracy comparison with previous studies described below:

Table 4.5: Model Accuracy Comparisons.

Authors	Model Used	Accuracy	Limitations
Balta et al. [1]	CNN	>99%	Data scarcity, "black-box" opacity, and limited labelled datasets
K. Duan et al. [3]	CNN	>96%	Need for standardized protocols, interoperability issues, lacking diversity
Kanupuru et al. [13]	YOLOv4 Tiny-YOLOv4	94% 87%	Small dataset, higher mis-classification for the lightweight model
Proposed Models	RF XGB LSTM	88% 82% 78%	×

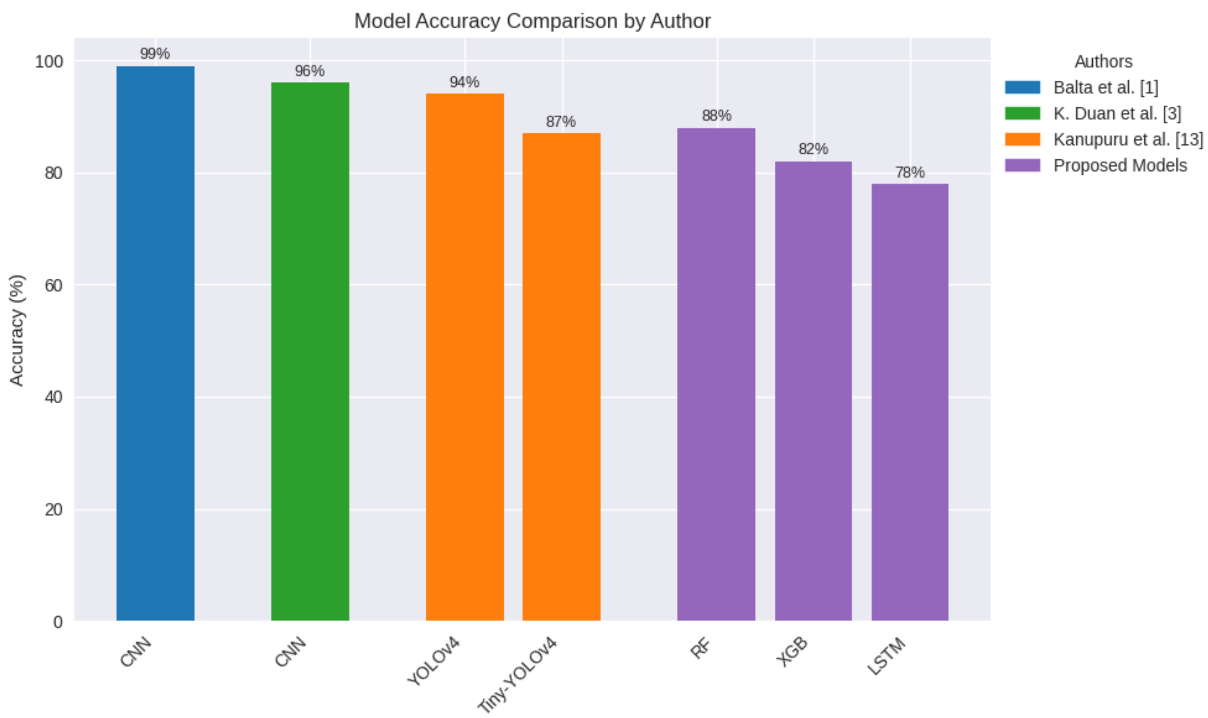


Figure 4.12: Model Accuracy Comparison Bar Diagram With Previous Works.

The proposed model is a hybrid combination of tree-based ensemble algorithms (Random Forest and XGBoost) and LSTM networks that can handle diverse sensor data, time variability in IoT networks, and visual and spectral characteristics. The hybrid model is easier to interpret and provides a strong edge on better deployment on the edge device when considered together with heavy convolutional neural networks (CNNs). The proposed model also utilizes diverse training paradigms on diverse datasets as opposed to previous work that was limited by small datasets and limited food types.

4.4.2 Blockchain For Product Authentication

We have compared Blockchain System in three different section with previous works.

A. Technical & System Components Comparative Analysis
B. B.Cost Comparison Analysis
C. C.Property Comparison Analysis

These comparison section has been described below.

A. Technical & System Components Comparative Analysis

In Table 4.6, a comparative analysis is presented. References [8], [14], [16], [17], along with the proposed system, employ blockchain-based approaches, while [20] relies on a centralized cloud model. The proposed system distinguishes itself by offering decentralized storage through IPFS and supporting dApps, features not observed in others.

Table 4.6: Technical & System Components Comparative Analysis.

Ref	Encryption Algorithm	Network	Storage System	Privacy	Online Time	Dapps	Implementation
Oh et al. [8]	ECDSA	Fabric	Immutable Ledger	High	Always Online	No	Prototype
A Singh et al. [14]	Keccak 256	P2P	Hybrid	Low	Always Online	Yes	Implemented
M. Tripoli [16]	SHA 256	Distributed Ledger	Not Available	Low	Not Stated	No	Conceptual
Y. P. Tsang et al. [17]	SHA 256	IOT Device	Hybrid	High	Always Online	No	Prototype
J. Wu et al. [20]	No	Cloud	Centralized	Low	Online	No	No
Proposed System	SHA 256	Decentralized	IPFS	High	Always Online	Yes	Prototype

In Table 4.6 the comparison between our proposed system is shown based on Encryption Algorithm, Networks, Storage system, Privacy, Online time, Dapps and Implementation.

B. Cost Comparison Analysis

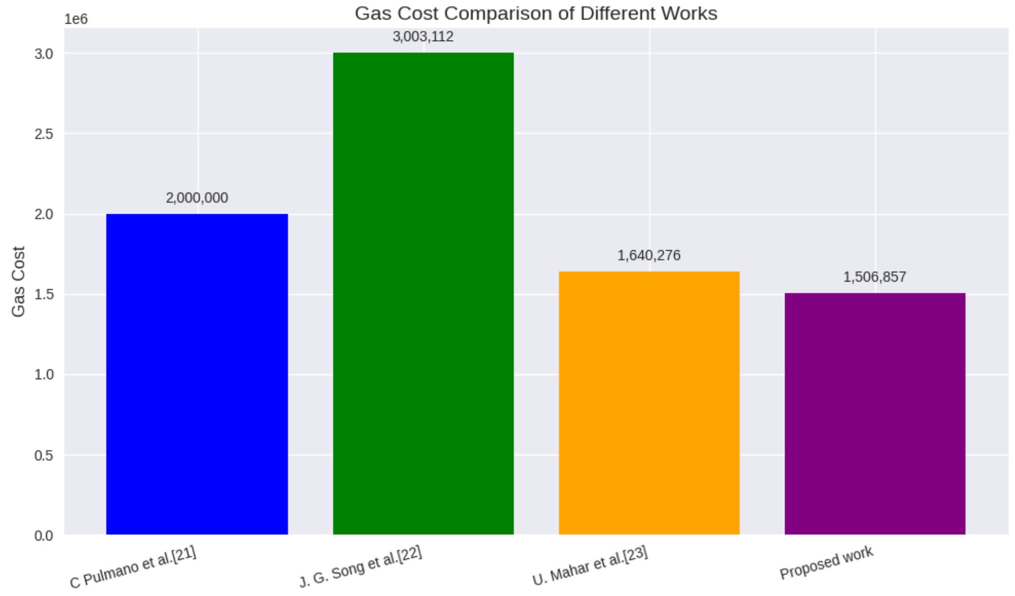


Figure 4.13 : Gas Cost Comparison Bar Diagram With Previous Works.

The comparison clearly shows that the cost of the proposed approach is the lowest, at 1,506,857, hence better than the rest of the previous works. This implies that J. G. Song et al. [22] have the highest cost of 3,003,112, followed by C. Pulmano et al. [21] at 2,000,000 and U. Mahar et al. [23] at 1,640,276. The proposed approach clearly shows the substantial reduction in the cost of computation, hence more cost-effective compared to all previous approaches in the blockchain environment.

C. Property Comparison Analysis

Table 4.7 illustrates the properties offered by our work and other existing research. Notably, all of the works mentioned in table offer immutability, transparency and security. Moving on to privacy and data integrity, papers [3], [4], [9], [14] mention while [16] only provides privacy. Lastly, only [3] provides accountability where this feature is unavailable in other previous works. However, our proposed work fulfills all six properties, including immutability, transparency, security, privacy, data integrity, and accountability for ensuring our work as better than the rest.

Table 4.7: Property analysis on some existing work

Reference	Immutability	Transparency	Security	Privacy Data	Integrity	Accountability
K. Duan et al. [3]	Yes	Yes	Yes	No	Yes	Yes
V. S. Hema et al. [4]	Yes	Yes	Yes	No	Yes	No
A S Patel et al. [9]	Yes	Yes	Yes	No	Yes	No
A Singh et al. [14]	Yes	Yes	Yes	No	Yes	No
M. Tripoli et al. [16]	Yes	Yes	Yes	Yes	Yes	No
Proposed system	Yes	Yes	Yes	Yes	Yes	Yes

i. Immutability

A transaction can neither be changed nor erased after it has been added to the blockchain. As a result, the system is invincible and the integrity of the data recorded on the blockchain is secured. Through cryptographic hashing and consensus methods, which guarantee that any effort to make changes to the blockchain will be rejected by the network. Immutability in the framework of product registration assures that registered product id cannot be altered or faked, giving stakeholders confidence that the data on them is correct and trustworthy.

ii. Transparency

The blockchain technology used is able to provide an open and transparent view of product registration information within the proposed food safety system. Information regarding all registered products, such as product number, brand, and production and expiration dates, along with an IPFS image link and aQR hash, is all recorded on the Ethereum blockchain and is able to be viewed by anyone. Through this, there is an increase in trust within the food system, as all entities have an accurate and immutable set of product information.

iii. Security

The proposed system takes advantage of the cryptographic principles utilized by the blockchain technology for providing a high-level secure framework for the authentication of products. The use of secure hashing algorithms, SHA-256, is applied for the hashing of the QR codes, while the decentralized consensus mechanism provided by Ethereum protects the data on the blockchain from unauthorized changes. Since the registration transaction is done using MetaMask wallets, the private keys aren't transmitted to the backend system.

iv. Privacy

The system ensures privacy for users by not storing personal or sensitive data in the blockchain. Also, the system interacts with the blockchain using crypt wallet addresses and not actual identities; this makes it possible for users to be pseudonymous. Additionally, the system stores the relevant data regarding the product on the blockchain and does not collect data from the users during the verification process when using the QR code.

v. Data Integrity

It also protects user privacy by not storing personal information on the blockchain. The user interacts with the blockchain, not by his identity but by wallet addresses, hence allowing for user privacy or anonymity. The system also stores information about products on the blockchain and does not collect user information during the verification process when the QR code is used.

vi. Accountability

Actually, blockchain technology provides a traceable and auditable environment where every registration transaction for a product is linked with a specific wallet address. It makes traceability possible, contributing towards accountability, wherein a party can track where every registered item comes from without requiring their personal identity information. Also, if there is illicit registration of a product, then its source can be traced back to a specific organization, preventing any harm in a trust-based approach for authenticating a product.

4.5 Summary

In this chapter, firstly the environment setup and hardware requirements for both AI and Blockchain was introduced. Then the model evaluation shows the different AI model's accuracy, recall and confusion matrix comparisons and how its working visualizing with its user interface. After that the blockchain system's workflow was discussed using web interface and showing the cost analysis for the system. Then both AI models and Blockchain features of our proposed system was compared to previous related works and showing our system's superiority. The findings show the successful integration of the AI component and the blockchain-based UI, facilitating the users in performing the two-layered process for freshness detection and product authentication.

Chapter 5

Engineering Standards and Design Challenges

This chapter describes the engineering standards, which directed the development process, focuses on the social and ethical aspects related to this work, and discusses sustainability, although alongside the system implementation challenges. Descriptions related to project management and financial analysis relevant to the integrated solution, which involves AI and Blockchain, will also be presented.

5.1 Compliance with the Standards

The system consists of three main modules:
AI image classification, blockchain product authentication, and QR customer verification. Therefore, the utmost adherence to software, hardware, and communication standards was mandatory to ensure reliability, security, and long-term maintainability for the system.

5.1.1 Software Standards

i. ISO/IEC 25010 — Software Quality Standards

Relevance: The relevance of the standard is for the implementation of the system to abide by the quality attributes defined, such as Reliability (consistent AI results), Security (tamper-evident blockchain), and Usability (user-friendly interface for the consumers).

ii. IEEE 830 — Requirements Specifications

Relevance: Used during requirements analysis to define requirements (for example, system shall use SHA-256 hashing for data hashing) and non-functional requirements (for example, system shall return results within 2 seconds).

iii. Solidity Security Standards (SWC Registry):

Relevance: The smart contract was developed using best practices in order to reduce possible weaknesses. Specifically, it made use of the Checks-Effects-Interactions pattern, which was helpful for protecting it from any kind of re-entrancy attacks, and it used standard types compatible with the Ethereum Virtual Machine (EVM).

iv. PEP 8 (Python Enhancement Proposals):

Relevance: Utilized for the AI and Backend development to ensure code readability, proper indentation, and modular structure in the Flask application and Machine Learning pipelines.

5.1.2 Hardware Standards

The system is designed to be hardware-agnostic regarding the end-user, but development adhered to:

ISO 12232 (Digital Still Cameras):

Relevance: The training of the AI relied on the standardization of the input images. To ensure the images taken by various smartphone cameras were compatible with the model trained on the dataset, the standard ISO speeds and exposure standards were followed on the Consumer Side.

5.1.3 Communication Standards

i. JSON-RPC (Remote Procedure Call):

Relevance: Used for communication between the Python Web3.py client and the Ethereum Sepolia Testnet nodes.

ii. HTTPS / TLS 1.2+:

Relevance: Ensured secure data transmission between the Flask web server, the Pinata IPFS gateway, and the user's client interface.

5.2 Impact on Society, Environment and Sustainability

5.2.1 Impact on Life

The overall impact of this technology on the life of the consumer would be the improvement of public health. This is because it provides consumers with an avenue to determine the spoilage of food through the use of artificial intelligence as well as confirming the expiry date of the food through blockchain technology. This helps to reduce the chances of diseases such as Salmonella and Escherichia coli.

5.2.2 Impact on Society & Environment

i. **Societal Impact:** It can be seen that the proposed system focuses on the very real issue arising in developing economies, which is the adulteration and counterfeiting of food. With the creation of an untamperable ledger, it helps to ensure the decreased distribution of counterfeits.

ii. **Environmental Impact:** Food waste is one of the biggest contributors to greenhouse gas emissions. By accurately evaluating the freshness level for the product and avoiding the sale of the item if it's not fresh in the initial stages of the supply chain, the system helps combat this problem.

5.2.3 Ethical Aspects

- **Data Integrity:** The system promotes ethical data management. This is achieved by utilizing blockchain technology. For instance, in most centralized systems, an administrator can modify the expiry dates of some products for the purpose of selling expired merchandise. However, utilizing blockchain technology makes such data immutable, thereby promoting ethical business practices.

- **AI Bias:** One of the primary moral issues considered within this paper is that of Dataset Bias. A significant amount of effort was placed into ensuring the "Fresh" and "Rotten" datasets included as large a variety of fruits and vegetables as possible to avoid the artificial intelligence system favoring the suppression of some types based simply on texture (for example, while differing lychees from rotting apples).

5.2.4 Sustainability Plan

- **Energy Efficiency:** The project uses the Sepolia Testnet and is compatible with the Proof-of-Stake consensus algorithm used in Ethereum, making the energy usage 99.9% lower compared to the Proof-of-Work algorithm used in previous blockchain networks.

- **AI Bias: Paperless Verification:** The system reduces the need for physical documentation with the implementation of product certificates/receipts in the form of QR code and blockchain hashes, which enhances environmental sustainability.

5.3 Project Management and Financial Analysis

The project was managed using Agile methodologies, allowing for iterative development of the AI models and Smart Contracts. Since this is an academic prototype, the direct costs were minimized. However, the table below projects the budget required for a real world commercial deployment.

5.3.1. Cost Analysis

Since this is an academic prototype, the direct costs were minimized. However, the table below projects the budget required for a real world commercial deployment.

Table 5.1: Cost Analysis

Component	Prototype Cost (Current)	Commercial Cost (Est.)	Rationale
Hosting (Server)	0 (Localhost)	50000 Taka	AWS/Azure for Flask backend & AI inference.
Blockchain Network	0 (Sepolia Testnet)	Variable (Gas Fees)	Deployment on Mainnet (Polygon/Ethereum) requires gas fees per transaction.
Storage (IPFS)	0 (Pinata Free Tier)	2200 Taka	Pinata Pro plan for faster pinning and larger storage.
Development	Student Time	120000 Taka	Salary for Blockchain & AI engineers.
Total	0	172200 Taka	Low operational cost makes it viable for SMEs.

This table shows the per section cost and total costing for the market deployment.

5.4 Complex Engineering Problem

5.4.1 Complex Problem Solving

This project addresses a **Complex Engineering Problem (CEP)** that requires resolving conflicting requirements between AI accuracy, Blockchain security, and system performance

Table 5.2: Mapping with Complex Engineering Problem.

EP1 Dept of Knowledge	EP2 Range Of Conflicting Requirements	EP3 Depth of Analysis	EP4 Familiarity of Issues	EP5 Extent of Applicable Codes	EP6 Extent Of Stake-holder Involvement	EP7 Interdependence
✓	✓		✓			✓

EP1: Depth of Knowledege Required-High: As envisioned, this whole system rests at a junction of AI research, cryptography, and distributed systems. Specifically related to the AI aspect of this work is the use of deep learning RF, XGB, LSTM architectures to assess how fresh a product is by analyzing images of them. The blockchain aspect rests on the use of crypto-hashing algorithms (SHA-256) and blockchain platforms and smart contracts to verify the authenticity of the data. But all of these components of this solution must work in concert. The key to building a secure solution end to end is recognizing how each of these components fits together.

EP2: Range of Conflicting Requirements-High: Although technologies for artificial intelligence and blockchain exist in their own right and are relatively mature, the combination for the detection of food freshness in a consumer application area has been relatively uninvestigated. There would appear to be an obvious novelty in terms of the engineering challenges posed by the combination of making predictions in an uncertain environment through AI and more deterministically through blockchain. The solution would appear to be an emerging application area in the engineering domain.

EP4: Familiarity of Issues-Low(Novelty): Though the technologies of artificial intelligence and blockchain are well established in themselves, their joint use in the detection of food freshness for consumer-level applications is rather unexplored. It is evident that the proposed solution offers new engineering challenges in terms of combining probabilistic AI predictions with deterministic techniques using blockchain and decentralized data access using IPFS. The lack of familiarity with the current exposure to the issues solved by the solution makes the solution a new and emerging engineering application area.

EP7: Interdependence-High: Moreover, the system is highly dependent on the various elements in the different subsystems. For instance, the effectiveness and accuracy of the AI component depend on the quality of the dataset and generalizability. Additionally, the effectiveness of the user interface depends on blockchain transaction delays and smart contract responsiveness. Also, the effectiveness of product authentication depends on the resources accessed through IPFS. Any problem or performance issue in one of the system elements can directly influence system effectiveness. Handling system level dependencies correctly entails rigorous architecture design and sensitivity to faults in the diverse technologies being used.

Mapping with Knowledge Profile

This section is designed to map the overall problem and **EP1** ***(multiple between K3, K4, K5, K6, K8 for attaining EP1)*** to the Knowledge Profile.

Table 5.3: Mapping with knowledge Profile.

K1	K2	K3	K4	K5	K6	K7	K8
Natural Science	Mathematics	Engineering Fundamentals	Specialist Knowledge	Engineering Design	Engineering Practice	Comprehension	Research Literature
		✓	✓	✓	✓		✓

K3: Engineering Fundamentals: Topics covered under this heading include the use of logic gates in programming, the use of cryptography hash algorithms and concepts of statistical probalities utilized in AI classification systems. These fundamentals provide the mathematical and theoretical basis required to design secure systems and build reliable predictive models.

K4: Specialist Knowledge: The key focus area of Machine Learning is related to RF, XGB and LSTM models. In regard to Blockchain technology, Gas and Consensus mechanisms, along with Solidity Bytecode are being focused upon. The specialist knowledge with enables efficient model training for different images while ensuring that smart contracts are optimized for cost, performance, and reliability on blockchain network.

K5: Engineering Design: This involves the concept of developing Dual Layer Architecture where artificial intelligence systems, as well as blockchain systems, run independently but provide the user with a combined output. This Separation improves scalability and security while allowing each layer to be upgraded or optimized without disrupting the other.

K6: Engineering Practice: This entails the use of version control with Git, contract testing via Remix IDE, and virtual environments for handling dependencies for python. These practices help maintain code integrity, enable safe collaboration, and ensure that smart contracts behave correctly before deployment. They also make development environments reproducible across team members, reducing configuration issues and unexpected runtime errors.

K8: Research Literature: Topics related to this work was researched and paper was studied. This work consists of previous literature's gap mitigation using more efficient techniques with the integration of AI and Blockchain.

5.4.2 Engineering Activities

Below, we describe a mapping of engineering tasks. For each mapping, we recommend subsections explaining the rationale behind it, as discussed in the table below.

Mapping with Complex Engineering Activities

This particular section aims to connect the broader issue with the different EA's.

Table 5.4: Mapping with Complex Engineering Activities.

EA1 Range of re-sources	EA2 Level of Interaction	EA3 Innovation	EA4 Consequences for society and environment	EA5 Familiarity
✓	✓	✓	✓	✓

E1: Range of Resources: The system also leveraged Python libraries such as TensorFlow, scikit learn, and OpenCV for model development and image processing. Additionally, smart contract development tools and blockchain frameworks were utilized to deploy and test the decentralized components effectively.

E2: Level of Interaction: These components communicate through APIs and smart contracts to ensure seamless data exchange and real time verification. The coordinated interaction enables secure product registration, image storage, freshness prediction, and instant retrieval of authenticated information for end users.

E3: Innovation: The innovation improves the aspect of food safety governance through the removal of the earlier role of the centralized authority in the process of food safety approval through the use of cryptographic proofs and AI analysis in place of the approval seal, which was unverified in the past.

E4: Consequences to Society/Environment: By enabling accurate food freshness detection, the system helps reduce the risk of foodborne illnesses and promotes safer consumption practices. Transparent product verification through blockchain strengthens consumer confidence and discourages the circulation of counterfeit or expired goods. Economically, this improves trust between producers, sellers, and consumers while supporting a more accountable and sustainable supply chain.

E5: Familiarity: Such integration requires an understanding of how blockchain networks are structured, how wallets are able to confirm the identity of users, and how the security of transactions is maintained. There is also the matter of synchronizing interactions between the interface, the logic on the servers, and the smart contract, together with the security of the information belonging to the users.

5.5 Summary

In this chapter, it is documented how the project complies with international standards of software development as well as hardware dev**No index entries found.**elopment (ISO 25010, IEEE 830). It also examines societal impact, specifically improvements made to health outcomes as well as the impact of fraud reduction. Finally, the project is aligned with Complex Engineering Problems (EP1 - EP7) and Activities, Knowledge Profile (K1-K8) and Complex Engineering Activities (EA1-EA5), thereby confirming the level of subject area expertise needed to combine AI, as well as blockchain, technologies.

Chapter 6

Conclusion

This chapter provides a summary of the salient results obtained from this project, along with the limitations faced during its development and further improvement prospects to extend its scope.

6.1 Summary

This project presented an integrated **AI Powered Food Freshness Detection With Blockchain Based Product Authentication**, designed to address two major real-world problems:

(i) Food freshness uncertainty for consumers and
(ii) Counterfeit product circulation.
The system integrates three key elements:

i. AI-Powered Food Freshness Detection

For this purpose, an image classification pipeline has been designed using the Long Short-Term Memory (LSTM) algorithm, Random Forest, XGBoost, and an ensemble classifier for voting out the best result. The pipeline classifies images into Fruits/Vegetables category with subcategories of Fresh and Rotten.

ii. Blockchain-Based Product Authentication (Sepolia Ethereum Testnet)

A custom-made smart contract in Solidity enables product registration on a blockchain. Then image storing using IPFS. Let product verification by QR code scanning and secure storage of product information and their hash values. The authentication of a product by a seller is done using MetaMask, while for a customer, it is done by scanning a QR code.

iii. Web-Based Hybrid Architecture

In an architectural implementation using a backend from Flask, there is utilization of an AI prediction API. Then IPFS uploads performed using Pinata from web. Web also let seller item submittal functionality and as well as customer verifications.
The UI provides a smooth user experience with features such as:

- AI Scanner
- Seller registration
- As well as QR verifications

Overall, this integrated system demonstrates how multiple technologies, such as decentralized identity management, AI decision support, and secure traceability, can be harnessed in a manner which positively impacts food safety.

6.2 Limitations

Although the system was successfully implemented, there were performance constraints:

i. Data Quality and Real-World Variability

The food images lacked adequate environmental variability in terms of lighting, season of the year, and background detail. Freshness indicators are slightly different, requiring vastly more data in order to reach above 90% accuracy.

ii. Limited Blockchain Transaction Speed

The registration process is dependent on network conditions on Sepolia Testnet.There may be variations in gas fees.

iii. Model Training Hardware Constraints

The training procedures were carried out on machines with limited CPU/GPU capabilities, thus limiting the complexity of the model and search space of hyperparameters.

iv. No Mobile App Yet

the moment, the system provides the customer with the browser interface only; otherwise, they have to use the webcam or the upload option.

v. Dynamic Sign-in

The system stil lacks Seller or Consumer different sign in and role based access.

6.3 Future Work

A number of approaches can significantly improve scalability, accuracy, and usability:

i. Advanced Deep Learning Models

Add EfficientNetV2, MobileNetV3, ResNet152, or Vision Transformers to reach over 95% accuracy. Expand the data range to include multi-class freshness classes besides the binary classification done in Fresh/Rotten.

ii. On-Chain Product Journey Tracking

On-chain product journey tracking will enable a transparent record of product transfer activities, ownership handovers, and document resales, while also incorporating critical supply chain metadata such as temperature and other conditions; together, these features allow consumers to verify the complete history of an item, including how many times it has been resold, ensuring trust and accountability across the supply chain.

iii. Mobile Application Development

Mobile application development using Flutter or React Native will make the system more user friendly.

iv. Real-Time IoT Sensor Integration:

This will use RFID tags, temperature sensors, and humidity monitors to continuously track product conditions, enabling proactive safety monitoring and ensuring that items remain within secure and reliable supply chain standards.

v. On-Chain AI Score Logging

This will provide a secure and immutable record of AI-generated evaluations, ensuring full auditability, transparency, and reliable dispute resolution by allowing stakeholders to verify and trust the decision-making process directly on the blockchain.

vi. Enhanced Security

Enhanced security in the system will be achieve through multi-signature product registration, ensuring that no single party can manipulate records; role-based access for sellers and inspectors, which enforces accountability and prevents unauthorized actions; and integration with Decentralized Identity (DID), providing verifiable digital identities that strengthen trust and safeguard the integrity of the supply chain.

vii. Marketplace Integration

Marketplace Integration An e-commerce platform where authenticated products are directly offered to customers by registered sellers.

References

[1] I. Balta, J. Lemon, C. A. Popescu, D. McCleery, T. Iancu, et al., “Food safety the transition to artificial intelligence (AI) modus operandi,” *Trends in Food Science & Technology*, vol. 165, Art. 105278, Nov. 2025.

[2] Q. Zhou, H. Zhang, S. Wang, *“Artificial intelligence, big data, and blockchain in food safety,”* International Journal of Food Engineering, vol. 2021, no. 29, 2021. DOI: 10.1515/ijfe-2021-0299.

[3] K. Duan, H. Onyeaka, G. Pang, Z. Meng, *“Pioneering food safety: Blockchain’s integration in supply chain surveillance,”* Journal of Agriculture and Food Research, vol. 2024, article 101281, 2024. DOI: 10.1016/j.jafr.2024.101281.

[4] V. S. V. Hema and A. Manickavasagan, “Blockchain implementation for food safety in supply chain: A review,” *Comprehensive Reviews in Food Science and Food Safety*, 2024.

[5] R. M. Ellahi, L. C. Wood, A. E.–D. A. Bekhit, *“Blockchain-Driven Food Supply Chains: A Systematic Review for Unexplored Opportunities,”* Applied Sciences, vol. 14, no. 8944, 2024. DOI: 10.3390/app14198944.

[6] M.-E. Dimitrakopoulou and A. Garre, “AI’s intelligence for improving food safety: only as strong as the data that feeds it,” *Current Food Science and Technology Reports*, vol. 3, no. 1, p. 15, May 2025.

[7] H. K. W. Aslam, F. Aslam, M. Aleem et al., “AI-driven food safety: transforming food inspection, traceability, and compliance in food industry and regulatory bodies: A mini review,” *Food Science & Applied Microbiology Reports*, vol. 3, no. 2, pp. 61-67, Nov. 2024.

[8] S. E. Oh, J.-H. Kim, J.-Y. Kim et al., “Food Safety Distribution Systems Using Private Blockchain: Ensuring Traceability and Data Integrity Verification,” *Foods*, vol. 14, no. 8, pp. 1405, Apr. 2025.

[9] A. S. Patel, M. N. Brahmbhatt, A. R. Bariya, J. B. Nayak, V. K. Singh, *“Blockchain technology in food safety and traceability concern to livestock products,”* Heliyon, vol. 9, no. e16526, 2023. DOI: 10.1016/j.heliyon.2023.e16526.

[10] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, “The rise of blockchain technology in agriculture and food supply chains,” *Trends in Food Science & Technology*, vol. 84, pp. 1-33, Sep. 2019.

[11] S. Jarka, *“Food safety in the supply chain using blockchain technology,”* Acta Scientiarum Polonorum – Oeconomia, vol. 18, no. 4, pp. 41-48, 2019. DOI: 10.22630/ASPE.2019.18.4.43.

[12] D. Bongarde, S. Pandit, and H. Pandit, “Use of Machine Learning and Artificial Intelligence in Food Spoilage Detection,” *International Journal of Engineering Research and Applications*, vol. 14, no. 4, pp. 79-85, Apr. 2024.

[13] P. Kanupuru, N. V. U. Reddy, *"A Deep Learning Approach to Detect the Spoiled Fruits,"* WSEAS Transactions on Computer Research, vol. 10, no. 10, 2022. DOI: 10.37394/232018.2022.10.10.

[14] A. Singh, A. Shenoy, and N. Thanekar, "Chain Thread: Blockchain-Powered Product Verification and Authenticity Tracking," *Int. J. for Research in Applied Science and Engineering Technology*, vol. 13, no. 4, pp. 8, Apr. 2025.

[15] J. Lin, Z. Shen, A. Zhang et al., "Blockchain and IoT based Food Traceability System," *Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly*, Singapore, 2021.

[16] M. Tripoli and J. Schmidhuber, "Emerging Opportunities for the Application of Blockchain in the Agri-food Industry," FAO & ICTSD, 2018.

[17] Y. P. Tsang, K. L. Choy, C. H. Wu, *"Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism,"* IEEE Access, vol. 7, pp. 129 000–129 015, 2019. DOI: 10.1109/ACCESS.2019.2940227.

[18] A. Pandey, W. Naikawadi, S. Patil et al., *"Fake Product Identification using Blockchain,"* Proceedings of the 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 1–5.

[19] Y. Zhao, H. Xu, and M. Chen, "Research and development of cloud-based food safety traceability system," *Adv. J. Food Sci. Technol.*, vol. 5, no. 12, pp. 1580-1583, Dec. 2013.

[20] J. Wu, L. Ping, X. Ge, Y. Wang, and J. Fu, "Cloud storage as the infrastructure of cloud computing," in 2010 International conference on intelligent computing and cognitive informatics, pp. 380–383, IEEE, 2010.

[21] C. Pulmano and P. Fernandez, *"Developing a Structural Standard for Smart Contract Electronic Health Records Based on the HL7 Fast Healthcare Interoperability Resources,"* in *Proc. 10th Int. Conf. Inf. Commun. Technol. for Ageing Well and e-Health (ICT4AWE)*, 2024, pp. 169-175.

[22] J. G. Song, E. Kang, H. W. Shin, and J. W. Jang, *"A Smart Contract-Based P2P Energy Trading System with Dynamic Pricing on Ethereum Blockchain," Sensors*, vol. 21, no. 6, Art. 1985, Mar. 2021.

[23] U. Mahar, M. Aleem, and E. Zahoor, "*TTECCDU: a blockchain-based approach for expressive authorization management," PeerJ Comput. Sci.*, vol. 9, e1212, Feb. 2023.

221-15-4673

ORIGINALITY REPORT

16%	11%	8%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	4%
2	Submitted to Muslim College Multan Student Paper	2%
3	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1%
4	Poonam Nandal, Mamta Dahiya, Meeta Singh, Arvind Dagur, Brijesh Kumar. "Progressive Computational Intelligence, Information Technology and Networking", CRC Press, 2025 Publication	<1%
5	journals.iium.edu.my Internet Source	<1%
6	Submitted to United International University Student Paper	<1%
7	ijees.net Internet Source	<1%
8	Shalli Rani, Ayush Dogra, Ashu Taneja. "Smart Computing and Communication for Sustainable Convergence", CRC Press, 2025 Publication	<1%
9	Helen Onyeaka, Adenike Akinsemolu, Taghi Miri, Nnabueze Darlington Nnaji et al. "Artificial intelligence in food system: Innovative approach to minimizing food	<1%

20% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

72 AI-generated only 20%
Likely AI-generated text from a large-language model.

0 AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.