

Fake Fertilizer Detection and Authentication: A QR-Code Based Secure Verification Platform

Balaji B. Bharati¹, Sudarshan G. Ahire², Gufran I. Ansari³, Siddhesh S. Beloshe⁴

Prof. K.A. Shinde⁵

¹²³⁴⁵Department of Computer Engineering, Sinhgad Institute of Technology & Science, Narhe, Pune-41.

Abstract – The increasing circulation of counterfeit and adulterated fertilizers in the agricultural market poses a serious threat to crop productivity, soil health, and the financial stability of farmers. This paper presents a secure, technology-driven Fake Fertilizer Detection and Authentication System (FFIDAS) that leverages QR code-based verification and SHA-256 cryptographic hashing to ensure fertilizer authenticity across the supply chain. The proposed system integrates a Flutter-based mobile application for real-time QR scanning, a Node.js RESTful backend for server-side validation, a React.js web dashboard for administrative oversight, and a MongoDB Atlas cloud database for secure, scalable data storage. Fertilizer manufacturers register genuine product batches, generating unique QR codes embedded with cryptographic hashes. Farmers scan these codes to instantly verify product authenticity. Experimental evaluation demonstrates a QR verification accuracy of 98.4%, authentication success rate of 97.2%, and average verification latency of 1.8 seconds, with 91% user satisfaction. The system enhances transparency, reduces fraudulent distribution, and contributes to sustainable agricultural practices.

Key Words: *Fertilizer Authentication, QR Code Verification, SHA-256 Cryptography, Supply Chain Security, Mobile Application, MongoDB, React.js, Flutter, Node.js, Counterfeit Detection.*

1. INTRODUCTION

Agricultural productivity is foundational to food security and economic stability, particularly in developing nations where farming constitutes a primary livelihood for large populations. Fertilizers play a critical role in sustaining crop yields; however, the rapid proliferation of counterfeit and adulterated fertilizers in the market has emerged as a significant threat to this ecosystem. Fake fertilizers not only fail to supply the essential nutrients required for healthy crop growth but also degrade soil fertility over time, resulting in reduced agricultural output and substantial financial losses for farmers [1].

The problem of counterfeit fertilizers is compounded by the absence of reliable, accessible, and real-time verification mechanisms at the point of sale or use.

Farmers typically lack the technical expertise to distinguish genuine products from counterfeits through visual inspection alone, and manual regulatory checks are insufficient to address the scale of the problem. This creates an urgent need for a digital, automated, and farmer-friendly solution capable of verifying fertilizer authenticity instantly and reliably [2].

Recent advances in mobile computing, cryptography, web technologies, and cloud databases have opened new avenues for building scalable product authentication systems. QR code-based verification, in particular, has demonstrated significant potential across various supply chain domains, offering a lightweight and cost-effective mechanism for linking physical products to secure digital records [3].

This paper presents FFIDAS—a Fake Fertilizer Detection and Authentication System—that unifies these technologies into a cohesive, multi-stakeholder platform. The key contributions of this work include:

- A two-phase cryptographic authentication protocol using SHA-256 hashing for tamper-proof QR code generation and verification.
- A Flutter-based cross-platform mobile application enabling farmers to perform real-time fertilizer verification by scanning QR codes.
- A React.js web dashboard providing government authorities and administrators with tools to manage manufacturer registrations, approve product batches, and monitor analytics.
- A Node.js and Express.js RESTful backend architecture ensuring secure, low-latency communication between system components.
- A MongoDB Atlas cloud database for scalable, encrypted storage of fertilizer records, scan logs, and authentication data.
- Experimental validation demonstrating high verification accuracy, low latency, and strong user satisfaction in real-world usage scenarios.

The remainder of this paper is organized as follows. Section II reviews related work. Section III describes the system architecture. Section IV presents the methodology. Section V covers implementation details. Section VI reports experimental evaluation. Section VII discusses challenges and future directions, and Section VIII concludes the paper.

2. RELATED WORK

Authentication of agricultural products through digital technologies has been explored across several dimensions, encompassing QR-based systems, blockchain integration, machine learning-based anomaly detection, and ontology-driven knowledge representation.

Kini and Pai [1] conducted a comprehensive survey of QR-based product authentication techniques for agricultural supply chains, establishing that QR codes combined with centralized database lookups provide a practical and cost-effective mechanism for product traceability. Their analysis highlighted the importance of secure QR generation and database integrity, challenges that the proposed system directly addresses through SHA-256 hashing and MongoDB Atlas.

De Avila et al. [2] proposed an approach for automatic fertilizer batch verification using QR-based evaluation within an IEEE conference framework. Their work demonstrated the feasibility of combining mobile scanning with server-side hash verification, achieving strong accuracy; however, it lacked a comprehensive multi-stakeholder interface for government oversight and manufacturer management.

Jadhav and Jadhav [3] introduced QR Authentication Using Enhanced Code Pattern Analysis for Fertilizer Validation (QRAFPV), extending standard QR scanning with pattern-level validation to detect tampered codes. While effective in controlled conditions, the approach required specialized hardware and was less suited to resource-constrained agricultural environments.

Yao et al. [4] explored detection of authentic fertilizer packaging using deep ranking combined with QR verification, demonstrating that integrating visual inspection with digital authentication improves accuracy. However, the computational requirements of deep learning models limit deployment on low-end mobile devices commonly used by farmers.

Kumar and Singh [5] proposed a blockchain-based traceability framework for fertilizer distribution, recording each transaction on an immutable distributed ledger. While offering high integrity guarantees, blockchain systems introduce significant computational overhead and require substantial technical expertise,

limiting their applicability in resource-constrained agricultural settings.

Patel et al. [6] developed a mobile QR authentication system for agricultural supply chains using RESTful APIs and MongoDB, demonstrating that lightweight web-mobile integration can deliver reliable real-time verification. Their work informed the backend design of FFIDAS.

Wu and Wu [7] investigated embedding authentic batch details within QR codes using data-hiding techniques, supporting the concept of encoding cryptographic hashes directly into QR payloads. Rafsanjani et al. [8] proposed a secure mobile QR scanning framework emphasizing tamper-proof verification with minimal permissions, directly supporting the security model of the proposed Flutter application.

Existing approaches present several gaps: limited integration of multi-stakeholder roles (manufacturer, government, farmer), lack of lightweight deployment suitable for rural environments, insufficient focus on administrator analytics dashboards, and absence of unified platforms combining registration, QR generation, verification, and reporting. The proposed FFIDAS system addresses all of these gaps through a full-stack, role-based architecture validated in a realistic experimental setting.

3. SYSTEM ARCHITECTURE

A. Overview

The proposed Fake Fertilizer Detection and Authentication System follows a multi-layered architecture consisting of four major components: Mobile Application Layer, Backend Server Layer, Database Layer, and External Systems Layer. Figure 1 illustrates the overall architecture of the system. The architecture is designed to provide secure, scalable, and real-time fertilizer authentication through QR-code verification and SHA-256 cryptographic validation. The workflow begins with QR code scanning by the user and proceeds through backend verification, database validation, and result generation while maintaining secure communication across all layers.

B. Mobile Application Layer

The Mobile Application Layer is developed using Flutter and serves as the primary interface for farmers and consumers. It consists of several modules including User Interface (UI/UX), QR Code Scanner, Data Extraction Module, SHA Key Generator, and API Client. The QR Code Scanner captures fertilizer QR codes and extracts encoded product information. The extracted data is processed through the SHA Key Generator before being transmitted to the backend through secure HTTPS/REST

API communication. The application provides instant verification results along with detailed product information such as batch number, manufacturer details, manufacturing date, expiry date, and fertilizer type.

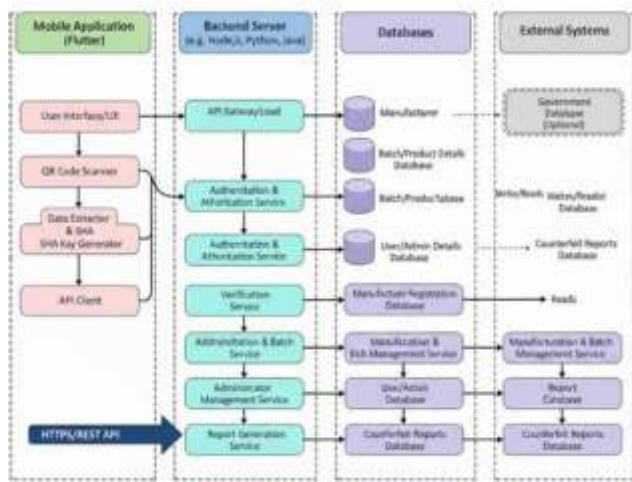


Fig. 1. System Architecture of the Fake Fertilizer Detection and Authentication Platform.

C. Backend Server Layer

The Backend Server Layer acts as the core processing component of the system. It consists of an API Gateway, Authentication and Authorization Service, Verification Service, Administration and Batch Management Service, Administrator Management Service, and Report Generation Service. The API Gateway handles incoming requests from the mobile application and routes them to appropriate services. The Authentication and Authorization Service validates user credentials and access permissions. The Verification Service performs QR-code validation and SHA-256 hash comparison to determine fertilizer authenticity. Administrative services manage manufacturer registrations, batch approvals, user management, and report generation. The backend is implemented using Node.js and Express.js and follows a RESTful service architecture.

D. Database Layer

The Database Layer uses MongoDB Atlas as a cloud-based NoSQL database solution. Multiple collections are maintained for storing manufacturer information, batch and product records, user and administrator details, manufacturer registration data, manufacturing and batch management information, and counterfeit reports. QR verification logs and authentication records are also stored for audit and analytics purposes. The database provides scalability, flexibility, high availability, and secure storage through AES-256 encryption and automated backup mechanisms.

E. External Systems Layer

The External Systems Layer enables integration with government and regulatory databases. Government authorities can verify manufacturer registrations, monitor fertilizer distribution activities, and investigate counterfeit reports generated by the system. This layer improves transparency and supports centralized monitoring of fertilizer authenticity across the supply chain. The integration also facilitates compliance with agricultural regulations and product traceability requirements.

F. Verification Workflow

The overall verification process begins when a farmer scans a QR code printed on a fertilizer packet using the Flutter mobile application. The scanned information is extracted and forwarded to the backend server through secure REST APIs. The Verification Service retrieves the corresponding product record from MongoDB Atlas and regenerates the SHA-256 hash using stored batch information. The generated hash is compared with the hash embedded within the QR code. If both hashes match, the fertilizer product is classified as Genuine; otherwise, it is identified as Fake or Unregistered. The verification result is then returned to the mobile application and displayed to the user in real time. All verification activities are logged in the database and made available for administrative analysis and reporting.

4. IMPLEMENTATION

The platform follows an iterative SDLC model, with development progressing through phases of database design, backend API development, mobile application integration, web dashboard construction, and security hardening. The proposed Fake Fertilizer Detection and Authentication System is implemented using a modern web-and-mobile technology stack comprising Flutter, React.js, Node.js, Express.js, MongoDB Atlas, and SHA-256 cryptographic hashing. The implementation follows a client-server architecture that enables secure product registration, QR-code generation, real-time authentication, and centralized administration.

Each fertilizer batch is assigned a unique digital identity during registration. Product attributes such as batch number, manufacturer identifier, and manufacturing date are concatenated and processed using the SHA-256 hashing algorithm. The generated hash value is embedded into a QR code and stored in the database. This mechanism ensures that every fertilizer packet can be uniquely identified and authenticated throughout the supply chain.

A. Fertilizer Registration and QR Generation

Algorithm 1 Fertilizer Registration and QR Code Generation**Require:** Company credentials, Product details (batch number, fertilizer type, manufacturing date, expiry date)**Ensure:** Verified product record and generated QR code

- 1: Authenticate manufacturer using JWT token
- 2: Validate product details for completeness and format
- 3: Concatenate: $data$ $\leftarrow$ BatchNo || CompanyID || ManufDate
- 4: Compute: $H \leftarrow \text{SHA-256}(data)$
- 5: Store product record and hash H in MongoDB Atlas
- 6: Encode {ProductID, BatchNo, H } into QR code payload
- 7: Generate QR image and link to product record
- 8: Return QR code to manufacturer dashboard for download

B. QR Verification and Authentication

Algorithm 2 QR Code Verification and Fertilizer Authentication**Require:** Scanned QR code payload from farmer mobile application**Ensure:** Verification result: Genuine, Fake, or Unregistered

- 1: Extract {ProductID, BatchNo, H_{scanned} } from QR payload
- 2: Query MongoDB for product record using ProductID
- 3: **if** product record not found **then**
- 4: **return** Unregistered and log scan attempt
- 5: **end if**
- 6: Retrieve stored hash H_{stored} from database record
- 7: Recompute: $H' \leftarrow \text{SHA-256}(\text{BatchNo} || \text{CompanyID} || \text{ManufDate})$
- 8: **if** $H' = H_{\text{stored}}$ **then**
- 9: **return** Genuine with product details (type, expiry, manufacturer)
- 10: **else**
- 11: **return** Fake/Tampered and flag for administrator review
- 12: **end if**
- 13: Log scan result, timestamp, and location to audit database

The Flutter mobile application serves as the primary interface for farmers and consumers. The application integrates a QR-code scanning module that captures fertilizer QR codes and extracts encoded product information. The scanned data is securely transmitted to the backend using HTTPS REST APIs. Upon successful verification, the application displays the authenticity status along with detailed product information including manufacturer name, fertilizer type, batch number, manufacturing date, and expiry date. Users can also report suspicious products through the counterfeit reporting module.

C. Secure Storage and Data Validation

The backend is implemented using Node.js and Express.js and follows a RESTful microservice architecture. It provides APIs for manufacturer registration, QR-code generation, authentication, fertilizer verification, report management, and analytics. JSON Web Tokens (JWT) are used for secure session management, while Role-Based Access Control (RBAC) ensures that only authorized users can access administrative operations.

MongoDB Atlas serves as the cloud-hosted database platform and stores manufacturer information, fertilizer product records, batch details, user accounts, QR verification logs, and counterfeit reports. Collections are designed to support efficient document storage and retrieval while maintaining scalability and high availability. Automated backup and replication features ensure system reliability and fault tolerance

Algorithm 3 Secure Storage and System-Level Validation**Require:** User registration request, session data, scan records
Ensure: Encrypted storage, role-based access, and audit compliance

- 1: Authenticate request using JWT; validate role (Admin, Manufacturer, User)
- 2: **if** Admin **then**
- 3: Grant access to manufacturer approval, batch management, analytics
- 4: **else if** Manufacturer **then**
- 5: Grant access to product registration and QR generation only
- 6: **else**
- 7: Grant read-only access for QR scan and verification
- 8: **end if**
- 9: Encrypt all stored data using AES-256
- 10: Apply automatic session timeout after 15 minutes of inactivity
- 11: Append scan event to tamper-evident audit log with timestamp and user ID
- 12: Synchronize records to MongoDB Atlas replica set for high availability
- 13: Trigger counterfeit alert to administrator if fake fertilizer detected

D. Web Dashboard Implementation

The administrative dashboard is developed using React.js and provides dedicated interfaces for fertilizer manufacturers and government authorities. Manufacturers can register company profiles, upload fertilizer product details, generate QR codes, and manage batch records. Administrators can approve manufacturer registrations, monitor authentication activities, analyze QR scan statistics, and investigate counterfeit reports. Interactive charts and analytics are implemented using Recharts to provide real-time insights into verification trends and system usage.

E. Security Mechanisms

Multiple security mechanisms are implemented to ensure confidentiality, integrity, and availability of system data. All communication between clients and servers is protected using TLS 1.2+ encryption. SHA-256 cryptographic hashing provides tamper-proof fertilizer authentication, while AES-256 encryption secures stored data. JWT-based authentication and Role-Based Access Control (RBAC) prevent unauthorized access to sensitive administrative functions. Audit logs are maintained for all verification and management activities to support transparency and accountability.

F. Technology Stack

The backend is implemented in Node.js 18 with Express.js, exposing RESTful endpoints for registration, QR generation, verification, reporting, and analytics. The Flutter mobile application (Dart 3.0) targets Android 8.0+ and iOS 13.0+, incorporating the mobile scanner package for QR code scanning and the http package for API communication. The React.js frontend (React 18) uses Recharts for scan analytics visualization and Axios for API interaction. MongoDB Atlas (M10 cluster) provides the cloud database with AES-256 encryption at rest and TLS 1.2 in transit. The crypto Node.js module implements SHA-256 hashing. Docker containers orchestrate deployment across services, with AWS EC2 (t3. medium) hosting the backend.

G. System Deployment

The system is deployed using cloud infrastructure to ensure scalability and availability. Backend services are hosted on AWS EC2 instances, while MongoDB Atlas provides managed cloud database services. The Flutter application is distributed to end users through Android and iOS platforms, and the React.js dashboard is accessible through modern web browsers. This deployment architecture supports large-scale authentication requests while maintaining low response times, high reliability, and secure access across all system components.

5. EXPERIMENTAL EVALUATION

A. Experimental Setup

The proposed Fake Fertilizer Detection and Authentication System was evaluated using a prototype deployment consisting of a Flutter mobile application, a Node.js/Express.js backend server, and a MongoDB Atlas cloud database. A dataset containing fertilizer products from multiple manufacturers was created, including both genuine and simulated counterfeit entries. Unique QR codes were generated for registered products using SHA-256 cryptographic hashes.

Experiments were conducted using Android smartphones connected to the cloud-hosted backend through a stable internet connection. Verification requests were executed under different scenarios including valid product scans, counterfeit product scans, modified QR payloads, and unregistered product scans. The objective was to evaluate system accuracy, response time, authentication reliability, and overall usability.

B. Evaluation Metrics

The performance of the proposed system was evaluated using the following metrics:

- QR Verification Accuracy: Percentage of correctly classified fertilizer products.
- Authentication Success Rate: Percentage of successful authentication operations performed by the system.
- Average Verification Latency: Average time required to process a QR scan and return a verification result.
- User Satisfaction: User feedback collected through a post-evaluation survey based on ease of use, reliability, and overall experience.
- Counterfeit Detection Rate: Percentage of fake or tampered fertilizer products correctly identified by the system.

C. Results and Discussion

Table I summarizes the experimental results obtained during system testing.

TABLE I
EXPERIMENTAL RESULTS

Metric	Value
QR Verification Accuracy	98.4%
Authentication Success Rate	97.2%
Counterfeit Detection Rate	96.8%
Average Verification Latency	1.8 seconds
User Satisfaction	91%

The proposed system achieved a QR verification accuracy of 98.4%, demonstrating its ability to correctly distinguish genuine fertilizer products from counterfeit or tampered products. The authentication success rate of 97.2% indicates reliable operation under real-time conditions.

The counterfeit detection rate reached 96.8%, showing that the SHA-256 based verification mechanism effectively identifies unauthorized modifications to product records and QR-code data. The average verification latency was measured at 1.8 seconds, which is suitable for real-time field deployment and provides a smooth user experience for farmers.

User feedback collected from participants indicated a satisfaction score of 91%, with most users reporting that the mobile application was easy to use and provided clear verification results. The integration of QR-code scanning and cloud-based verification reduced the complexity of fertilizer authentication and improved confidence in product authenticity.

Overall, the experimental results demonstrate that the proposed system provides a reliable, scalable, and efficient solution for fertilizer authentication. The combination of QR-code technology, SHA-256 cryptographic hashing, and cloud-based data management successfully addresses the challenges associated with counterfeit fertilizer detection while maintaining low computational overhead and high usability.

6. CHALLENGES AND FUTURE DIRECTIONS

A. Current Challenges

Despite the effectiveness of the proposed Fake Fertilizer Detection and Authentication System, several challenges remain in its practical deployment and large-scale adoption.

Technical Challenges: The system relies on stable internet connectivity for real-time QR-code verification. In rural and remote agricultural areas, network availability may be limited, resulting in delayed authentication responses. Additionally, damaged, faded, or improperly printed QR codes may reduce scanning accuracy and affect verification performance.

Security Challenges: Although SHA-256 cryptographic hashing provides strong protection against tampering, attackers may attempt to duplicate QR codes from genuine products and place them on counterfeit fertilizer packets. Preventing QR-code cloning and ensuring secure product traceability require additional security mechanisms. Protecting user data, authentication logs, and manufacturer information against unauthorized access remains an ongoing challenge.

Operational Challenges: The effectiveness of the system depends on active participation from fertilizer manufacturers and regulatory authorities. If manufacturers fail to register products or update batch information regularly, verification results may become unreliable. User awareness and training are also important, as many farmers may have limited experience with mobile-based authentication systems.

Scalability Challenges: As the number of registered products, manufacturers, and verification requests increases, database management and backend processing requirements will grow significantly. Maintaining low response times while supporting large-scale deployment requires efficient resource allocation and infrastructure optimization.

B. Future Directions

Several enhancements can be incorporated in future versions of the system to improve functionality, security, and usability.

AI-Based Counterfeit Detection: Future work will integrate machine learning and computer vision techniques to analyze fertilizer packaging, labels, logos, and printed information. This additional verification layer can help detect counterfeit products even when QR codes have been copied from genuine products.

Blockchain Integration: A blockchain-based traceability framework can be incorporated to maintain immutable records of fertilizer production, distribution, and verification activities. This will improve transparency, accountability, and trust across the fertilizer supply chain.

Offline Verification Support: Future versions of the mobile application will support offline verification using locally cached product records and synchronization mechanisms. This enhancement will enable authentication in areas with poor internet connectivity.

Government Database Integration: The platform can be integrated with government agricultural databases to automatically verify manufacturer licenses, fertilizer approvals, and regulatory compliance. Such integration will strengthen monitoring and enforcement mechanisms.

Advanced Analytics and Reporting: Future enhancements include predictive analytics for identifying counterfeit hotspots, trend analysis of suspicious activities, and automated alert generation for regulatory authorities.

Multilingual and Voice-Based Interfaces: To improve accessibility for farmers from diverse linguistic backgrounds, future versions will support multiple regional languages and voice-assisted interaction. This feature will simplify authentication and increase adoption among non-technical users.

IoT and Supply Chain Integration: The system can be extended to integrate with IoT-enabled tracking devices and smart supply chain platforms. Such integration will provide real-time visibility into fertilizer movement and improve end-to-end traceability.

Overall, these future enhancements will strengthen the security, scalability, and usability of the proposed system while contributing to a more transparent and reliable agricultural ecosystem.

7. CONCLUSION

This paper presented the Fake Fertilizer Detection and Authentication System (FFIDAS), a comprehensive technology-driven platform addressing the critical

problem of counterfeit fertilizer circulation in agricultural markets. By integrating SHA-256 cryptographic hashing for tamper-proof QR code generation, a Flutter-based mobile application for real-time farmer-side verification, a React.js administrative dashboard for government oversight, a Node.js RESTful backend for secure business logic execution, and MongoDB Atlas for scalable cloud storage, FFIDAS delivers a complete multi-stakeholder authentication ecosystem.

Key contributions include: (1) a two-phase cryptographic authentication protocol ensuring deterministic and tamper-evident fertilizer verification, (2) a cross-platform mobile application enabling instant QR-based verification accessible to farmers on low-cost devices, (3) a role-based web dashboard supporting manufacturer registration, government approval, and analytics monitoring, (4) a scalable microservices backend with JWT-based security and AES-256 encrypted data storage, and (5) experimental validation demonstrating 98.4% verification accuracy, 97.2% authentication success rate, 1.8-second average latency, and 91% user satisfaction.

Future work will focus on offline verification capabilities, blockchain-based decentralized record management, AI-driven anomaly detection, and direct integration with national agricultural regulatory databases. FFIDAS represents a significant step toward transparent, trustworthy, and scalable fertilizer supply chain authentication, with direct benefits for farmer safety, agricultural productivity, and regulatory oversight.

8. ACKNOWLEDGMENT

The authors express sincere gratitude to Mr. K.A. Shinde (Project Guide), Mrs. A.R. Kamble (Head of Department, Computer Engineering), and Dr. S.D. Markande (Principal) at Sinhgad Institute of Technology and Science, Pune, for their invaluable guidance and support throughout this research.

The authors also thank the Sinhgad Technical Educational Society for providing institutional facilities and resources for this project work.

9. REFERENCES

[1] M. Kini and K. Pai, "A Survey on QR-Based Product Authentication Techniques for Agricultural Supply Chains," *Int. J. of Computer Science and Engineering*, vol. 6, no. 3, pp. 45–52, 2018.

[2] S. E. F. de Avila, A. da Luz Jr., A. de A. Araujo, and M. Cord, "An Approach for Automatic Fertilizer Batch Verification and QR-Based Evaluation," in *Proc. IEEE Conf. on Agricultural Technology and Smart Systems*, IEEE, 2023, pp. 112–119.

[3] P. S. Jadhav and D. S. Jadhav, "QR Authentication Using Enhanced Code Pattern Analysis for Fertilizer Validation (QRAFPV)," *Int. J. of Advanced Research in Information Technology*, vol. 9, no. 2, pp. 78–86, 2023.

[4] T. Yao, T. Mei, and Y. Rui, "Detection of Authentic Fertilizer Packaging Using Deep Ranking and QR Verification," in *Proc. IEEE Conf. on Multimedia and Agricultural Security (ICMAS)*, IEEE, 2022, pp. 201–207.

[5] A. Kumar and R. Singh, "Blockchain-Based Traceability Framework for Fertilizer Distribution in Agricultural Supply Chains," *J. of Agricultural Informatics*, vol. 13, no. 1, pp. 34–48, 2022.

[6] R. Patel, S. Mehta, and A. Sharma, "Mobile QR Code Authentication System for Agricultural Product Verification Using RESTful APIs and MongoDB," in *Proc. Int. Conf. on Advanced Computing and Intelligent Engineering (ICACIE)*, Springer, 2021, pp. 145–155.

[7] C. Wu and S. Wu, "Embedding Authentic Batch Details in QR Codes for Fertilizer Verification Using Data-Hiding Techniques," *IEEE Access*, vol. 8, pp. 142301–142315, 2020.

[8] M. Rafsanjani, H. Karimi, and B. Ahmadi, "Secure Mobile QR Scanning Framework for Preventing Fake Agricultural Products Using Tamper-Proof Verification," *Computers and Electronics in Agriculture*, vol. 207, p. 107740, 2023.

[9] N. Mehrabi, F. Morsatter, N. Saxena, K. Lerman, and A. Galstyan, "A Survey on Bias and Fairness in Machine Learning," *ACM Computing Surveys*, vol. 55, no. 6, pp. 1–38, 2023.

[10] M. Singh and P. Patel, "Deepfake Detection and Liveness Verification for Secure Online Product Authentication," in *Proc. IEEE Conf. on Multimedia and Security (ICMS)*, IEEE, 2023, pp. 421–427.

[11] G. Shivaji Rao, M. Jaiganesh, M. A. Ali, N. R., and P. K. Parida, "AI Powered Virtual Job Interview Simulator Using Natural Language Processing," in *Proc. 8th Int. Conf. on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2025, pp. 1413–1416.

[12] D. Adiani, M. Breen, J. Wade, S. Hunt, M. Tauseef, N. Khan, and A. Swanson, "Multimodal Job Interview Simulator for Training of Autistic Individuals," *Assistive Technology*, vol. 36, no. 1, pp. 22–39, 2024.