Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

AUREL:AI-Driven Blockchain Platform for Authentic Product Verification and Trusted Recommendations

Sugantha Lakshmi R.[1], Abirami K.[2], Harini P.[3], Jeya Keerthana M.[4]

Department of Computer Science and Engineering, Saranathan College of Engineering (Autonomous), Tiruchirappalli, India.

E-mail: [1]suganthalakshmi7127@saranathan.ac.in, [2]cse251002@saranathan.ac.in, [3]cse251035@saranathan.ac.in, [4]cse251046@saranathan.ac.in

Abstract

The widespread use of fake cosmetic and personal care products has become a threat to consumer safety and product authenticity. Traditional verification methods such as QR codes, holograms, and centralized database are vulnerable to duplication and manipulation. To overcome these issues, this paper proposes AUREL, an AI-enabled blockchain platform for authentic product verification and recommendations. The proposed AUREL framework consists of product registration with blockchain, AI-based product visual verification, behavioral scan analytics, and recommendation service. In the developed application framework, first, manufacturers register the product information with a hash code generated by cryptographic technique. Second, consumers scan QR codes and take pictures of packages of the products through a mobile application for verification. Third, the system validates the blockchain and analyses the authenticity of the product to identify the unusual verification activities. A decision fusion algorithm is used to combine the outputs of each verification layer to classify products as genuine, suspicious, or fake. Finally, when fake products are found, the recommendation system suggests verified alternative products to the consumers. The proposed solution has been experimentally evaluated with a product verification success rate of 98.4%.

DOI: https://doi.org/10.36548/jaicn.2026.3.003
Extended version of article received from **6th International Conference on Artificial Intelligence, 6G Communications and Network Technologies 2026**
Received: 06.05.2026, received in revised form: 09.06.2026, accepted: 01.07.2026, published: 10.07.2026

Keywords: Product Authenticity Verification, Fake Detection, Computer Vision, Blockchain, Behavioral Scan Analytics, Recommendation System.

1. Introduction

The fast development of e-commerce and digital retail platforms has made cosmetic, skin care, and personal care products widely available to the people. Nevertheless, this rapid proliferation of fake products also enables serious threats to customer safety, brand reputation, and supply chain integrity. Fake cosmetic products usually have unauthorized components or even dangerous materials included into their formulas.

Authentication techniques like QR Codes, bar codes, holograms, and central verification databases have significantly enhanced product traceability. Although these methods have been widely adopted, they also come with certain restrictions. Product codes can be replicated, labels can be duplicated, and databases can also be manipulated. The present authentication methods have not succeeded in offering a Corruptproof mechanism for dealing with the fake products problem in a distributed environment.

Recent innovations in the blockchain have offered capabilities of decentralized and tamper-proof record keeping systems that help trace the products with better transparency. The use of the distributed ledger in recording information about products allows securing provenance validation while protecting the data from any changes in the registered records. Whereas, AI and computer vision technologies have shown their effectiveness in analysis of the packaging, logos, labels, and visual attributes of the products for identification purposes. While the technologies have proven themselves separately, most of the existing systems utilize one of these approaches.

Additionally, traditional authentication mechanisms are mainly concentrated on verifying product details while ignoring user interaction data that can indicate the existence of fake distribution networks. The analysis of abnormal scanning, multiple verification requests, and peculiar geographical accesses can offer some useful signals for identifying possible fake distributions. Moreover, most of the current authentication schemes do not have an option to guide users towards verified substitutes.

To address these issues, this research study proposes AUREL, an AI-enabled blockchain-based platform for product authentication and recommendation. The developed

system architecture includes product registration using blockchain, AI-driven visual product verification, behavioral scan analysis, and recommendation engine as one single solution. Blockchain technology will be used for creating the permanent identity of each product using cryptographic hashing, whereas AI-based image processing will perform verification based on visual similarity of the scanned product against the registered reference. Furthermore, behavior analysis will help in understanding the patterns related to verification process, which will be further classified as genuine, suspicious, and fake through decision fusion.

The main contributions of this work are summarized as follows:

- AUREL offers an integrated platform that integrates a decentralized blockchain-powered product registration system with an artificial intelligence-based visual authentication process.
- Scan-based behavioral analysis to detect any irregularities in the verification process which might signify the presence of fake products is part of the solution.
- A consumer-centric decision framework for consumers through offering verified product recommendations in case of unusual products.

The remainder of this paper is organized as follows. Section 2 provides an overview of the existing studies on authentication using blockchain, fake detection, and recommendation systems. Section 3 introduces our proposed framework, AUREL. In Section 4, we discuss the experiment results and performance analysis. Finally, Section 5 concludes the paper and mentions some potential future work.

2. Related Works

The increasing prevalence of fake products has motivated researchers to incorporate technologies such as blockchain, artificial intelligence, and recommendations to enhance the user trust on cosmetics. In recent years, there have been efforts to apply these technologies but mostly separately rather than combining them into one approach.

Gupta et al. [1] have developed a fake product identification framework for Small and Medium Enterprises using blockchain technology to deal with fakes in the supply chain. This solution applies Hyperledger blockchain technology, QR code product tracing, and cloud storage to enable small and medium enterprises to verify their products. Researchers have also

proved that blockchain technology could contribute to traceability and minimize the spread of fake products but they did not offer any recommendation features for users. Pillai et al. [2] proposed the blockchain-based product identification framework, where the product details were stored and verified through the distributed ledger. This method increases transparency and protects from any changes in the product data. However, the absence of analytical tools for evaluation of user feedback and customer preferences is notable. Rathod et al. [3] have built a blockchain based model for detecting fake products which stores product transactions in the distributed ledger and allows customers to authenticate the products using the provided user IDs. This study also has made use of the advantages of immutability and security of the blockchain technology in preventing the usage of fake products. Yet, the framework focuses only on validating the supply chain and not on dealing with trust problems associated with reviews or recommendations. Anusha et al. [4] have developed a hybrid e-commerce trust framework by integrating the product recommendation and fake review detection. The model uses sentiment analysis, machine learning models and anomaly detection technique to detect fake reviews.

Varghese et al. [5] used artificial intelligence to identify fake products using machine learning techniques. It shows how effective artificial intelligence can be in identifying suspicious attributes of products to differentiate real and fake products. Despite its efficiency, the developed framework does not use any modern technologies to store the user data securely and reliably. Shah et al. [6] explored the challenges in the validation and verification process of AI products in the regulated industry, such as the healthcare sector and medical devices. It highlights the need for reliable and transparent AI systems. Nevertheless, the presented research study lacks the information about fake product detection and decentralized verification approaches. Saraswathi et al. [7] examined the application of blockchain technology to counteract fake goods and increase consumer trust. The framework employs distributed ledgers to provide transparent history of the product in order to make the entire supply chain process traceable. Although this framework was successful in providing traceability and authenticity of the product, it does not have any intelligent recommendation system or consumer sentiments analysis tool. Lyu et al. [8] designed an artificial intelligence framework that improves consumer trust by personalizing their services based on sentiment analysis. It analyzes the opinion of the customer and their behavior to provide better recommendations.

Gao et al. [9] have developed a product authentication and traceability architecture using blockchain technology, which will record the product life cycle information. This research has shown the application of blockchain technology in assuring the data integrity and transparency of the product provenance. but, the main limitation of this research is that it provides a traceability framework without any intelligent recommendation features for consumers. Prokipchuk et al. [10] have suggested an intelligent blockchain-based framework for verifying the authenticity of products. A distributed blockchain-based product verification approach was suggested by Kumar et al. [11] to combat fake products in supply chains. The solution relies on unchangeable blockchain-based data to facilitate secure product authentication and traceability among various participants. Even though the solution enhances transparency and product verification, it lacks the AI-based mechanism for the assessment of trustworthiness and personalized recommendations. Reviewing the effect of the genuineness of reviews on the trust of customers in e-commerce websites is the main objective of Kori et al. [12]. It becomes apparent from their research that legitimate product reviews play an important role in the purchase decision-making process of consumers.

Although significant progress has been made in using blockchain technology for fake detection and AI for increasing trust, current research works still examine these problems separately. While blockchain applications concentrate on the traceability and authentication of products, the application of AI is mainly connected with the accuracy of recommendations and reviews. The proposed AUREL framework incorporates the following elements into one system: product authentication using blockchain technology, visual verification by means of artificial intelligence, behavioral scan analytics, and recommendations.

3. Proposed Methodology

The proposed AUREL framework, blockchain technology, artificial intelligence, and behavioral analysis have been combined into a secure and reliable platform for identifying fake products and making recommendations. The system modules include product registration, blockchain database, multiple levels of verification, decision making process, product classification, and recommendations. The entire process starts from the product registration by the manufacturers and ends with verification and recommendations to consumers.

The developed AUREL framework utilizes the detailed products datasets available on the Kaggle platform [13] to perform the following operations: product registration, blockchain-

based authentication and Dependable recommendations. The dataset includes more than 9,000 product instances belonging to over 30 different retail product categories, including cosmetics, skincare, personal care, household essentials, electronics, fashion, and grocery items. Each record contains structured product attributes such as Product ID, Product Name, Brand Name, Category, Price, Product Description, Customer Rating, and Stock Information, providing comprehensive metadata for efficient product management and recommendation services. Before proceeding with the product registration operation in the blockchain, key attributes related to products, such as Product ID, Brand Name, Batch Number, Manufacturing Date, and Expiry Date, were extracted to calculate the SHA-256 Hash for each product. The obtained data is then stored securely in the Hyperledger Fabric blockchain. For the product authentication phase, the QR code was used in order to check the product information recorded in the blockchain and for the recommendation module to use other attributes and generate appropriate recommendations based on the category, authenticity, rating and popularity. The dataset was further pre-processed by removing duplicate entries, handling missing values, and standardizing categorical attributes to improve data consistency. The variety and scale of the dataset enables comprehensive evaluation of blockchain-enabled product verification and trusted recommendation under realistic retail scenarios, at the same time ensuring reproducibility of the experimental results.

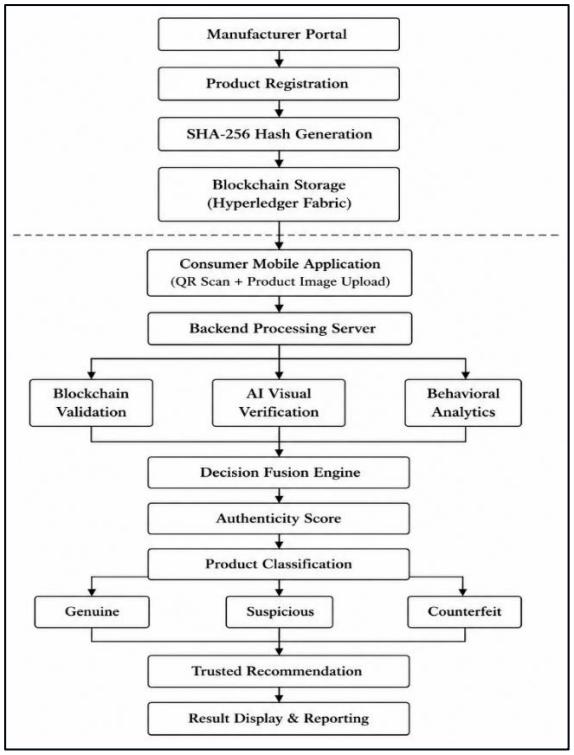

Figure 1. Architecture of the proposed AUREL framework

3.1 Product Registration and Blockchain Storage

The product information is initially registered via the Manufacturer Portal. Authorized manufacturers submit product details including Product ID, Product Name, Brand Name, Batch Number, Manufacturing Date, and Expiry Date.

To create a tamper-resistant digital identity, a SHA-256 cryptographic hash is generated using the registered product attributes:

$$H = SHA256(PID \,||\, BN \,||\, MD \,||\, ED \,||\, BR) \quad (1)$$

where PID denotes Product ID, BN represents Batch Number, MD represents Manufacturing Date, ED represents Expiry Date, and BR denotes Brand Name.

The calculated hash value is stored in the hyperledger fabric blockchain using smart contracts. Since blockchain records are immutable and decentralized, unauthorized modifications to registered product information are restricted. This process implements trusted product provenance and traceability throughout the product lifecycle.

3.2 Consumer Verification Process

Consumers conform the products using the mobile application by scanning the product QR code and uploading a packaging image. The QR code contains encoded product information link to the blockchain record.

The scanned data and uploaded image are transferred to the Backend Processing Server, which coordinates all verification activities. The backend continuously initiates blockchain validation, AI-based visual verification, and behavioral analytics.

3.3 Blockchain Validation

The Blockchain Verification module rebuilds the product hash from the scanned QR code information and compares it with the corresponding hash stored on the blockchain ledger.

The reconstructed hash code corresponds with that on the blockchain, the product is then verified using blockchain technology. Otherwise, it means there could be duplication of the product or fake manufacturing of the product.

The blockchain validation score is represented as:

- $B = 1$, if blockchain record matches
- $B = 0$, otherwise

This verification layer ensures data integrity and product traceability.

3.4 AI-Based Visual Verification

The uploaded image of the product is analysed by the AI Visual Verification component. Initially, the picture goes through pre-processing procedures such as resizing, normalization, and denoising.

The AI model extracts multiple visual features including:

- Logo structure
- Label alignment
- Typography consistency
- Color distribution
- Packaging design patterns

The features extracted are compared against the images of the reference products that are available in the verification database. This is used to compute the confidence level (A) that the product is genuine.

Higher similarity scores indicate genuine products, whereas significant deviations indicate fake characteristics.

3.5 Behavioral Analytics

The Behavioral Analytics module continuously monitors consumer verification activities to identify unusual product distribution patterns.

$$S = \alpha F + \beta R + \gamma G + \delta T \quad (2)$$

where:

- F = scan frequency score

- R = repeated scan score
- G = geographic anomaly score
- T = temporal anomaly score

The following behavioral parameters are analyzed:

- Scan frequency
- Repeated scan attempts
- Geographic scan distribution
- Time-based access patterns
- Historical verification records

Abnormal scanning behavior may indicate fake product distribution. Based on the observed patterns, a behavioral risk score (S) is generated and forwarded to the decision-making layer.

3.6 Decision Fusion and Authenticity Scoring

The outputs calculated from Blockchain Validation, AI Visual Verification, and Behavioral Analytics are integrated within the Decision Fusion Engine.

The final authenticity score is computed as:

$$AS = W_b B + W_a A + W_s S \tag{3}$$

where:

- AS = Authenticity Score
- B = Blockchain Validation Score
- A = AI Verification Score
- S = Behavioral Analytics Score
- W_b, W_a, and W_s are weighting coefficients assigned to each verification layer.

The equal weighting coefficients of 0.33 were assigned to each verification layer initially. The values of these weights may vary depending on the needs of the application. The evidence combination is done by decision fusion to enhance the classification robustness.

3.7 Product Classification

Based on the calculated authenticity score, products are categorized into three classes:

- Genuine Product (AS ≥ 75)
- Suspicious Product (50 ≤ AS < 75)
- Fake Product (AS < 50)

The classification module determines the final verification outcome presented to consumers.

3.8 Trusted Recommendation and Reporting

When the product is suspected of being fake, the Trusted Recommendation system will be activated. The recommendation engine will search for products from the same category or brand using verified blockchain information and recommend them in order of authenticity, ratings, and popularity.

$$RS = \lambda A_v + \mu P + \nu R \tag{4}$$

where:

- A_v= authenticity score
- P= popularity score
- R= user rating score

In addition, fake reports can be submitted via the mobile application. The logs, scanning history, and user report are saved for future analysis by manufacturers and regulatory authorities. Lastly, the results of the verification along with the recommendations are conveyed to the end-user via the Result Display and Reporting module.

4. Results and Discussion

The performance of the developed AUREL approach was analyzed by the blockchain validation, visual verification by artificial intelligence, behavior analysis, and trusted recommendation generation. The experimental results prove the ability of the proposed approach to authenticate real products, recognize suspect products, detect fake products, and offer trusted alternative products. The verification results are presented in Figures 2–4, whereas the performance results are provided in Table 2.

4.1 Software Tools and Implementation Environment

Table 1 summarizes the software tools and technologies used to implement the developed AUREL framework. The Flask technology serves as the backend controller responsible for product registration, blockchain communications, AI-based product authentication, and recommendations, with the Hyperledger Fabric providing the necessary security for the authentication process. TensorFlow and OpenCV perform image-based authentication, while the MySQL database is responsible for storing product metadata and verification history. The implemented integration provides a means of coordinating the operation of all components of the system, and achieves an average verification speed of 1.8s per product.

Table 1. Software tools and technologies used for framework implementation

Component	Software / Tool
Frontend Interface	HTML5, CSS3, JavaScript, Bootstrap
Backend Framework	Flask (Python 3.11)
Blockchain Platform	Hyperledger Fabric 2.5
Cryptographic Algorithm	SHA-256
AI Framework	TensorFlow 2.15
Image Processing	OpenCV 4.9
Data Processing	NumPy, Pandas
Recommendation Module	Scikit-learn
Database	MySQL 8.0
Development Environment	Visual Studio Code

Operating System	Windows 11
Hardware Configuration	Intel Core i7 Processor, 16 GB RAM

4.1 Genuine Product Verification

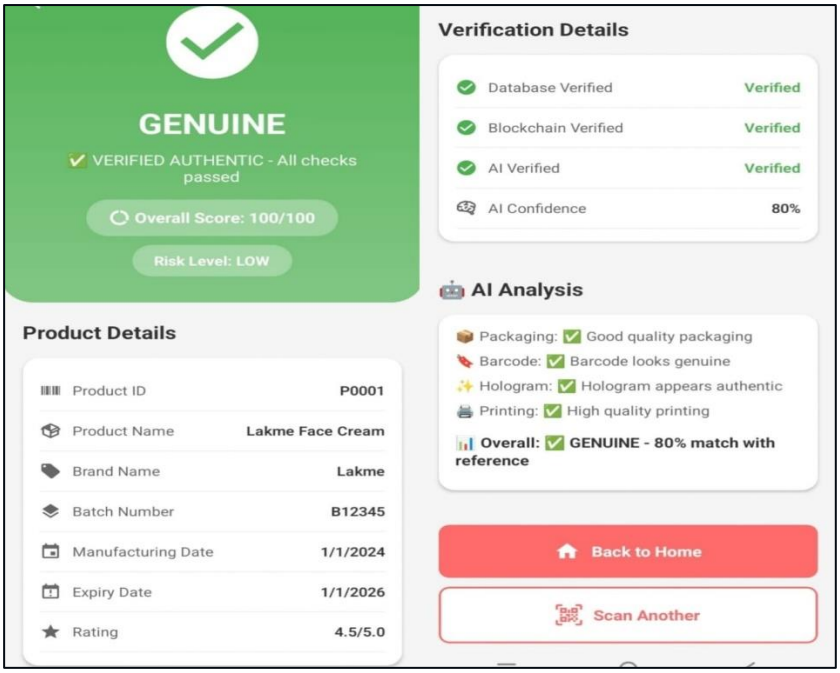

Figure 2. Blockchain-enabled genuine product verification

Figure 2 illustrates the verification result of an authentic product enrolled into the blockchain network. While the verification, there was a match between the QR code data and the blockchain data with a reliability of 99.1% of validation using the blockchain technology. At the same time, the AI Visual verification module verified the packaged product against the reference product images with 97.8% accuracy.

The behavioral analytics module captured typical user scanning patterns without deviations or anomalies in behavior patterns. The combined results from the three verification modules were analyzed through the decision fusion engine, leading to an excellent score on product authenticity and the product was classified as genuine. This successful verification helped in contributing to the Product Verification Success Rate of 98.4% and End-to-End Verification Efficiency of 97.2%.

4.2 Suspicious Product Detection

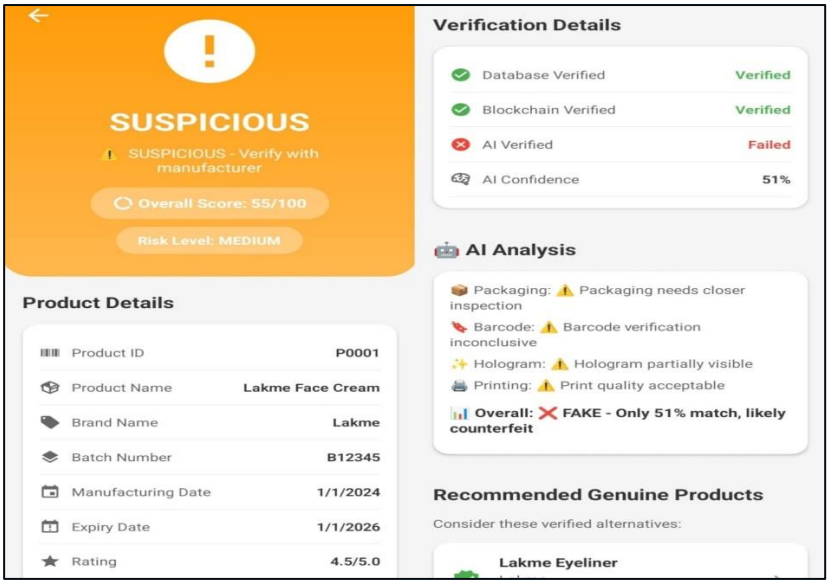

Figure 3. AI-based suspicious product identification

Figure 3 shows a verification scenario in which the product was classified as suspicious. Although the successful identification of the product using blockchain validation, discrepancies arose during visual and behavioral verification processes. The AI algorithm showed moderate discrepancies in packaging attributes such as label positioning, logo design, and patterns from the registered reference picture.

4.3 Fake Product Detection and Trusted Recommendation

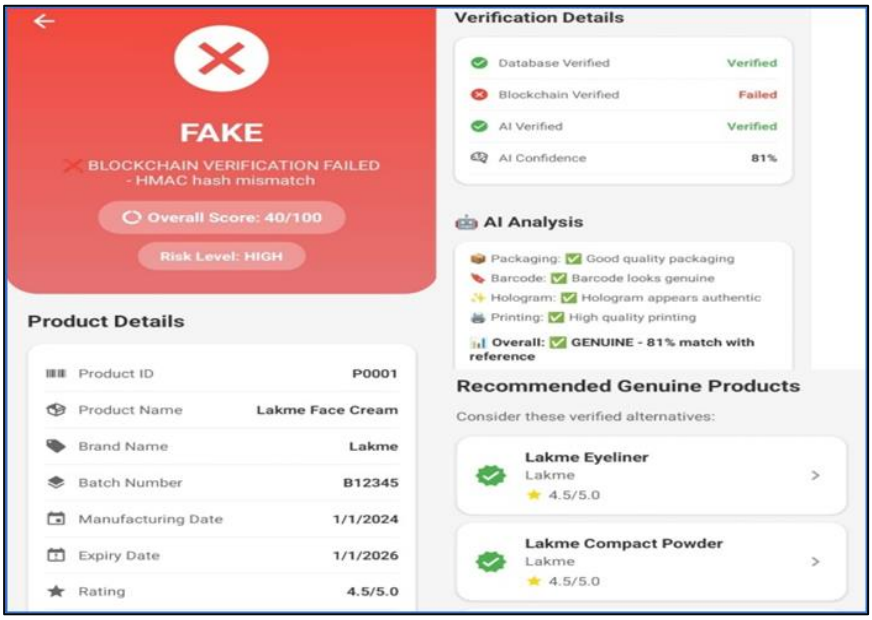

Figure 4. Fake product detection with verified product recommendations

The verification result of a fake product is provided in Figure 4. Here, the verification process through the blockchain validation module finds inconsistencies between the scanned information of the product and the corresponding blockchain entry, suggesting the possibility of tampered or duplicated products. Additionally, the AI-based visual verification module finds major discrepancies between the uploaded packaging picture and the genuine, with a lower similarity score.

The behavioral analytics engine also detected abnormal verification patterns associated with fake product circulation. After analyzing all these factors using the decision fusion engine, a low authenticity score was obtained, and the product was categorized as a fake. The proposed system successfully detected fake products with a rate of 96.9%.

After the process of detecting any possible fakes, the Trusted Recommendation module was initiated to provide help for customers in finding other authentic alternatives of the products stored in the blockchain. The recommendation engine provided Trusted Recommendation Relevance of 95.8%, which guarantees the high degree of relevance and authenticity of recommended products.

4.4 Overall System Performance Analysis

Table 2. Performance evaluation of the proposed AUREL framework

Performance Metric	Value
Product Verification Success Rate	98.4%
Blockchain Validation Reliability	99.1%
AI Visual Verification Confidence	97.8%
Behavioral Risk Detection Rate	95.6%
Decision Fusion Consistency	97.4%
Fake Detection Success Rate	96.9%
Trusted Recommendation Relevance	95.8%
Consumer Verification Satisfaction	96.3%
Average Verification Response Time	1.8 s
End-to-End Verification Efficiency	97.2%

Table 2 presents an overview of the performance results of the AUREL framework. The Product Verification Success Rate is 98.4%, proving that the proposed combination of

blockchain authentication, image verification based on AI, and behavioral analysis has proven to be effective. The reliability of Blockchain Validation is 99.1%.

The AI Visual Verification Confidence of 97.8% indicates that the image verification component has been able to differentiate between genuine and fake packaging features. Similarly, the Behavioral Risk Detection Rate of 95.6% affirms that the system has been capable of detecting risky user behavior and fake distribution patterns. The Decision Fusion Consistency of 97.4% shows that the multi-level verification architecture is capable of fusing evidence from various verifications.

The proposed framework scored 96.3% in terms of consumer verification satisfaction, which reflects positive user experience in the verification process. Additionally, the Average Verification Response Time of 1.8 seconds also proves the efficiency of the framework for real-time authentication. All the above results clearly show that the proposed AUREL framework is indeed an efficient and reliable platform to verify products and generate recommendations.

5. Conclusion

The proposed AUREL is an AI-driven blockchain platform designed for authentic product verification and trusted recommendation generation. The developed framework has integrated blockchain technology product registration, AI-powered image verification, behavioral scan analysis and decision fusion techniques. The use of this framework would enable product authentication through blockchain traceability, AI image verification and behavior analysis. Also, recommendations about alternatives to suspicious or fake products are provided using the recommendation module. It should be noted that the integration of these layers of verification increases performance in fake detection and improving consumer confidence in product authenticity. Future work will concentrate on the adoption of more sophisticated deep learning algorithms for improved visual validation performance, expanding the framework for use in multiple product types, in addition to the implementation of IoT-based supply chain tracking to facilitate real-time product traceability in commercial environments.

References

[1] Gupta, Sangeeta, Ramu Kuchipudi, Md Sohail, Karan Singh, J. Mahalakshmi, and Ashok Sarabu. “Fake Product Identification for Small and Medium Firms (FPISMF) Using Blockchain Technology.” Measurement: Sensors 2024, vol 33: 101164.

[2] Pillai, Anuradha, Pranitha Sukumar, Sanjana Mohite, Archana Vanniyar, and Kalyani Pampattiwar. “Identifying Fake Products Using Blockchain.” In Proceedings of the International Conference on Emerging Trends in Industry 4.0 Technologies (ICETI4T) 2025: 1-5

[3] Rathod, K. K., A. Katageri, A. T. Chetana, A. Tandle, and A. B. Kumar. "Detection of Fake Product Using Blockchain." Indiana Journal of Multidisciplinary Research 2024, vol 4, no. 3: 118-121.

[4] Anusha, Poranki, Buse Sudeep Sahas, and T. Lakshmi Surekha. "Enhancing E-Commerce Trust: An Integrated Product Recommendation and Fake Review Detection System." In International Conference on Data Science and Network Engineering, Cham: Springer Nature Switzerland, 2025: 25-35.

[5] Varghese, Richu Jacob, Shilpa Shaji Nellikkakunnel, and Sruthy Sunilkumar. "An AI-Based Fake Products Identification System.”, 2022: 1-16

[6] Shah, Nirali. "Validation and Verification of Artificial Intelligence Containing Products Across the Regulated Healthcare or Medical Device Industries." International Journal of Science and Research (IJSR) 2024, vol 13, no. 7: 66-71.

[7] Saraswathi, S., J. Suresh, and D. M. Gandhi. "Combating Fake Products with Blockchain Technology to Enhance Trust and Authenticity in Consumer Markets." Indian Journal of Science and Technology 2024, vol 17, no. 34: 3512-3521.

[8] Lyu, Guiying, and Ahmad Yahya Dawod. "AI-Driven Consumer Trust Enhancement in E-commerce: A Dynamic Sentiment-Based Marketing Framework for Cross-Platform Personalization." In Proceedings of the 2025 16th International Conference on E-business, Management and Economics, 2025: 289-293.

[9] Gao, Xiao, Wenyin Zhang, Bin Zhao, Jiqun Zhang, Jiuru Wang, and Yilong Gao. "Product Authentication Technology Integrating Blockchain and Traceability Structure." Electronics 2022, vol 11, no. 20: 3314.

[10] Prokipchuk, Oleh, Lyubomyr Chyrun, Myroslava Bublyk, Valentyna Panasyuk, Viktor Yakimtsov, and Roman Kovalchuk. "Intelligent System for Checking the Authenticity of Goods Based on Blockchain Technology." In MoMLeT+ DS, 2021: 618-665.

[11] Kumar, V. Ajay, Mohan Krishna Sadi, K. Sai Krishna, D. Devi Satya, M. Bhaskar, and U. Vinay. "A Novel Strategy for Product Verification via Decentralized Blockchain Networks." In 2025 6th International Conference on Recent Advances in Information Technology (RAIT), IEEE, 2025: 1-7.

[12] Kori, Geetesh Kumar, and Neeraj Kumar Sharma. "The Role of Review Authenticity in Building Consumer Trust: A Study on Product Reviews.", International Journal of Science and Management Studies (IJSMS), 2025, vol 8, no. 1: 87-89.

[13] Sujay Kapadnis, Detailed Products Datasets. Kaggle Dataset. Available: https://www.kaggle.com/datasets/sujaykapadnis/products-datasets?resource=download