IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14638

End to End Tracking and Authentication of Drugs

Shubham Rathod[1], Gaurav Talekar[2], Akshay Pundekar[3], and Samarth Pandhare[4]

Department of Computer Engineering Sinhgad Institute of Technology and Science (SITS)

Savitribai Phule Pune University, Pune, Maharashtra, India[1,2,3,4]

Abstract: Counterfeit medicines are a serious threat to health-care safety because they may contain incorrect ingredients, wrong dosage, harmful substances, or no active medical component. Traditional medicine verification methods mainly depend on manual checking of packaging, batch numbers, expiry dates, and seller trust. However, these methods are not always reli-able because counterfeiters can duplicate medicine labels and packaging. This paper presents the design and development of MedSecure Guardian, a web-based fake medicine detection and authentication system using QR code verification. The proposed system allows users to scan a QR code or enter medicine details manually and verify the medicine record from a secure database. The system is implemented using React, Vite, TypeScript, Tail-wind CSS, shadcn/ui, Supabase, and QR scanner integration. It provides quick authentication results such as genuine, suspicious, or not found. The system is designed for patients, pharmacists, healthcare workers, and medicine distributors to provide a first-level digital verification layer. The proposed framework improves accessibility, reduces manual verification effort, and supports safer healthcare practices by helping users identify suspicious medicines before use.

Index Terms: Fake Medicine Detection, Counterfeit Medicine, QR Code Verification, Medicine Authentication, Healthcare Se-curity, Supabase, React, Web Application

I. INTRODUCTION

Medicines play an important role in healthcare and disease treatment. The quality and authenticity of medicines directly affect patient safety. However, counterfeit medicines have become a major issue in the healthcare sector. Fake medicines may appear similar to original medicines, but they may contain wrong ingredients, incorrect dosage, harmful substances, or no active ingredient. Such medicines can lead to treatment failure, serious health problems, and loss of trust in healthcare systems.

In many places, patients and pharmacists do not have a simple and reliable method to verify whether a medicine is genuine or fake. Most users depend on packaging, batch number, expiry date, brand name, and seller trust. These methods are not sufficient because counterfeiters can copy the physical appearance of medicine packaging.

Quick Response (QR) codes are widely used in prod-uct identification, payment, advertising, access control, and healthcare-related applications. QR codes can store product-specific information and can be scanned easily using smart-phones or web applications. However, QR-based systems also require proper security because malicious QR codes and fake links may mislead users.

To address the issue of counterfeit medicine verification, this paper proposes MedSecure Guardian, a web-based fake medicine detection and authentication system. The system allows users to scan a medicine QR code or manually en-ter medicine details. The input is verified against medicine records stored in the database. The system then displays the authentication result to the user.

The main contribution of this paper is the development of a practical, web-based digital medicine verification system that can be accessed through a browser. The system is designed to be simple, responsive, and useful for patients, pharmacists, and healthcare workers.

II. LITERATURE REVIEW

Recent studies focus on QR code security, QR code data reliability, healthcare fraud detection, and abnormal behavior analysis. These areas are related to the proposed MedSecure Guardian system because the project uses QR-based verifica-tion and healthcare-related authentication.

The reviewed papers show that QR codes are useful for authentication but require secure scanning and reliable data handling. Healthcare fraud detection studies also show that suspicious activities can be identified using data-driven tech-niques. Based on these observations, MedSecure Guardian focuses on a practical QR-based medicine verification system that can be extended in the future with suspicious scan analysis and advanced counterfeit detection.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14638

III. PROBLEM STATEMENT

Counterfeit medicines are difficult to identify using only physical inspection. Patients, pharmacists, and healthcare workers may not always have access to laboratory testing or official verification systems. Manual checking of packaging, batch number, and expiry date is not fully reliable because counterfeiters can duplicate labels and medicine packaging.

There is a need for a digital system that allows users to verify medicine authenticity quickly using QR code scanning or medicine details. The system should be easy to use, secure, responsive, and accessible through a web browser.

Therefore, the problem is to design and develop a web-based fake medicine detection and authentication system that can:

1) Verify medicine authenticity using QR code or manual input.
2) Store medicine records securely in a database.
3) Provide instant verification status to users.

1) Help patients and pharmacists identify suspicious medicines.

TABLE I
LITERATURE REVIEW OF EXISTING SYSTEMS

S No	Title	Author	Year	Method/Methodology Used	Result/Conclusion
1	QsecR: Secure QR Code Scanner According to a Novel Malicious URL De-tection Framework	Ahmad Sahban Rafsanjani, Norshaliza Binti Kamaruddin, Hazlifah Mohd Rusli, Mohamma d Dabbagh	2023	Malicious URL detection using blacklist, lexical, host-based, and content-based features. The system used predefined static feature classification for secure QR scanning.	The system achieved 93.50% de-tection accuracy and 93.80% preci-sion. This work shows that QR code scanning requires security checks to avoid malicious or fake links.
2	Covert Communication via the QR Code Image by a Data Hiding Technique Based on Module Shape Adjustments	Da-Chun Wu and Yuan-Ming Wu	2020	QR code image processing and data hiding using module shape adjust-ments while maintaining QR code readability.	The study explains QR code struc-ture, readability, and error correction. It supports the importance of reliable QR code design for authentication-based systems.
3	Medicare Fraud Detection Using Graph Analysis: A Comparative Study of Ma-chine Learning and Graph Neural Networks	Yeeun Yoo, Jinho Shin, Sunghyon Kyeong	2023	Graph analysis, graph centrality measures, machine learning mod-els, and graph neural networks for healthcare fraud detection.	The study shows that healthcare fraud detection can be improved by analyzing relationships between providers, physicians, and benefi-ciaries. This supports future suspi-cious activity analysis in MedSecure Guardian.
4	Abnormal Group-Based Joint Medical Fraud Detection	Chenfei Sun, Zhong-min Yan, Qingzhong Li, Yongqing Zheng, Xudong Lu, Lizhen Cui	2019	Abnormal group mining using per-son similarity adjacency graph and group classification for medical fraud detection.	The method improves the detection of suspicious groups and helps re-duce false positives. It is useful for future detection of suspicious verifi-cation patterns.

IV. KEY LIMITATIONS OF EXISTING SOLUTIONS

Current medicine verification and QR-based authentication systems suffer from several limitations:

1) **Manual Verification Dependency:** Many users still depend on manual checking of packaging, batch number, expiry date, and seller trust, which may not detect counterfeit medicines accurately.
2) **Lack of Centralized Digital Verification:** There is often no simple centralized web platform where users can verify medicine details instantly.
3) **QR Code Security Issues:** QR codes can be misused by attackers or counterfeiters. Fake QR codes may redirect users to malicious or incorrect information.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14638

4) **Limited Accessibility:** Some verification systems are company-specific or region-specific and may not be easily accessible to all patients and pharmacists.

5) **No Suspicious Activity Analysis:** Many systems do not analyze repeated failed scans, duplicate medicine IDs, or suspicious verification patterns.

6) **No Real-Time User-Friendly Result:** Users need a sim-ple interface that clearly displays whether the medicine is genuine, suspicious, or not found.

V. PROPOSED SYSTEM OVERVIEW

The proposed MedSecure Guardian system is designed as a web-based fake medicine detection and authentication platform. It helps users verify whether a medicine is genuine or suspicious by using QR code scanning and database verifi-cation.

The platform primarily serves patients, pharmacists, health-care workers, and medicine distributors. A user can open the MedSecure Guardian website through a browser and use the verification feature. The user can either scan the QR code printed on the medicine package or manually enter medicine details such as medicine ID, batch number, or code value.

After the input is submitted, the system checks the entered or scanned value against the medicine records stored in the Supabase database. If a matching valid record is found, the system displays the medicine as genuine. If no valid record is found, the system displays a suspicious or not found message. The system also includes an admin-side medicine man-agement module. Admin users can add, update, or remove medicine records. This ensures that medicine data can be maintained in a structured and secure way.

The proposed system uses React, Vite, TypeScript, Tailwind CSS, shadcn/ui, Supabase, and QR scanner integration. React is used to build the user interface, Supabase is used for database management, and the QR scanner is used for fast medicine code scanning.

VI. SYSTEM ARCHITECTURE / METHODOLOGY

The MedSecure Guardian system follows a modular and scalable architecture that integrates frontend, QR scanning, database verification, and result generation. The system is designed to provide a fast and simple medicine verification process.

A. Architecture Overview

The system consists of the following major components:

1) Frontend Layer: The frontend is developed using React, Vite, TypeScript, Tailwind CSS, and shadcn/ui. It provides the interface for users to scan QR codes, enter medicine details, and view verification results.

2) QR Scanner Layer: The QR scanner layer allows users to scan QR codes using the camera of their mobile phone or laptop. The scanned QR value is passed to the verification module.

3) Backend and Database Layer: Supabase is used as the backend database service. It stores medicine records such as medicine name, batch number, manufacturer, expiry date, QR code value, and medicine status.

4) Verification Layer: The verification layer compares the scanned or manually entered medicine details with existing database records. Based on the match, the system generates a result.

5) Result Display Layer: The result display layer shows the final medicine authentication status to the user. The result can be genuine, suspicious, or not found.

B. Architecture Flow

The sequential workflow and data propagation mapping within the system architecture are detailed chronologically below:

User / Patient / Pharmacist

↓

React Web Interface

↓

QR Scan or Manual Medicine Input

↓

Supabase Database Verification

↓

Authentication Result

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14638

C. *Methodology / Workflow*

The working of the system can be described in the following steps:

1) User opens the MedSecure Guardian website.
2) User selects QR scan or manual verification option.
3) User scans the QR code or enters medicine details.
4) The frontend validates the input.
5) The system sends the verification request to Supabase.
6) Supabase checks the medicine record.
7) The system receives the verification response.
8) The result is displayed as genuine, suspicious, or not found.

D. *Key Features of Methodology*

- QR-code-based medicine verification.
- Manual medicine search option.
- Secure medicine record storage.
- Fast authentication result.
- Responsive web interface.
- Admin-side medicine data management.

VII. Implementation Details

The implementation of MedSecure Guardian is divided into multiple modules.

A. *User Module*

The user module allows patients, pharmacists, and health-care users to access the website and verify medicine authenticity. Users can scan a QR code or manually enter medicine details.

B. *QR Scanner Module*

The QR scanner module uses the device camera to scan QR codes. It reduces manual input and makes medicine verification faster.

C. *Medicine Verification Module*

This module compares the scanned or entered data with medicine records stored in the database. If the medicine record exists and is valid, the system displays it as genuine. If no valid record is found, the system displays a suspicious or not found message.

D. *Admin Module*

The admin module can be used to manage medicine records. Admin users can add, update, or delete medicine details.

E. *Database Module*

The database module stores medicine-related information. Supabase is used for database management and backend support.

TABLE II
Sample Medicine Database Fields

Field Name	Description
medicine_id	Unique medicine identification number
medicine_name	Name of the medicine
batch_number	Batch number of the medicine
manufacturer	Name of the manufacturer
expiry_date	Expiry date of the medicine
qr_code_value	Unique QR code value
status	Genuine or suspicious status
created_at	Record creation date

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14638

VIII. ALGORITHM

The fundamental verification procedural execution sequence is structured as follows:

1) Start.
2) Accept medicine ID, batch number, or QR code value.
3) Validate the input.
4) Send the input to the Supabase database.
5) Search for a matching medicine record.
6) If the record exists and the status is valid, display "Genuine Medicine".
7) Otherwise, display "Suspicious or Not Found".
8) Stop.

IX. RESULTS AND DISCUSSION

The system was tested using different inputs such as valid medicine details, invalid medicine details, valid QR code values, invalid QR code values, and empty inputs. The system successfully displayed appropriate verification results based on the database records.

TABLE III
TEST CASES AND RESULTS

Test Case	Input	Result
Valid medicine search	Correct medicine ID	Pass
Invalid medicine search	Wrong medicine ID	Pass
QR scan test	Valid QR code	Pass
Invalid QR scan	Wrong QR code	Pass
Empty input test	Blank field	Pass
Responsive test	Mobile screen	Pass

The result shows that the proposed system can provide quick first-level medicine verification. The use of QR scanning improves usability and reduces manual input errors. The web-based design makes the system accessible from mobile phones, tablets, and desktop browsers.

X. ADVANTAGES

The proposed system has the following advantages:

- Provides fast medicine verification.
- Reduces dependency on manual checking.
- Supports QR-code-based authentication.
- Provides a simple and responsive user interface.
- Can be accessed through a web browser.
- Useful for patients, pharmacists, and healthcare workers.
- Supports secure medicine record management.

XI. LIMITATIONS

The proposed system has some limitations. It requires an internet connection to verify medicine records. The system depends on accurate medicine data entered by authorized users. It cannot physically test the chemical composition of medicine. QR codes may also require stronger security methods to prevent copying or misuse.

XII. FUTURE SCOPE

The system can be improved in the future by adding:

- Blockchain-based medicine supply chain tracking.
- AI-based fake packaging detection using image process-ing.
- Manufacturer dashboard.
- Pharmacy dashboard.
- Mobile application.

DOI: 10.17148/IJIREEICE.2026.14638

- SMS-based verification.
- Real-time suspicious medicine reporting.
- Analytics dashboard for repeated fake medicine scan attempts.

XIII. CONCLUSION

MedSecure Guardian represents a practical digital solution for fake medicine detection and authentication. The system addresses the limitations of manual medicine verification by using QR code scanning and database-backed authentication. It allows users to verify medicine authenticity quickly through a web-based interface.

By using React, Vite, TypeScript, Tailwind CSS, shadcn/ui, Supabase, and QR scanner integration, the system provides a modern and responsive platform for medicine verification. The proposed system helps patients, pharmacists, and healthcare workers identify suspicious medicines before use.

The system acts as a first-level authentication layer and cannot replace laboratory testing. However, it provides an effective and accessible method for digital medicine verification. In the future, the system can be enhanced with blockchain-based supply chain tracking, AI-based packaging detection, mobile application support, and suspicious scan analytics.

REFERENCES

[1] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, "QsecR: Secure QR code scanner according to a novel malicious URL detection framework," *IEEE Access*, vol. 11, pp. 92523–92538, 2023, doi: 10.1109/ACCESS.2023.3291811.

[2] D.-C. Wu and Y.-M. Wu, "Covert communication via the QR code image by a data hiding technique based on module shape adjustments," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 12–34, 2020, doi: 10.1109/OJCS.2020.2984473.

[3] Y. Yoo, J. Shin, and S. Kyeong, "Medicare fraud detection using graph analysis: A comparative study of machine learning and graph neural networks," *IEEE Access*, vol. 11, pp. 88278–88295, 2023, doi: 10.1109/ACCESS.2023.3305962.

[4] C. Sun, Z. Yan, Q. Li, Y. Zheng, X. Lu, and L. Cui, "Abnormal group-based joint medical fraud detection," *IEEE Access*, vol. 7, pp. 13589–13596, 2019, doi: 10.1109/ACCESS.2018.2887119.

[5] React, "React Documentation." [Online]. Available: https://react.dev/

[6] Supabase, "Supabase Documentation." [Online]. Available: https://supabase.com/docs

[7] Vite, "Vite Documentation." [Online]. Available: https://vitejs.dev/

[8] Tailwind Labs, "Tailwind CSS Documentation." [Online]. Available: https://tailwindcss.com/docs