INTERNET OF THINGS

Design and Implementation of a Bi-Modal QR Code and Scratch-Code Drug Authentication System for Pharmaceutical Verification in Nigeria

Oghenetega Avwokuruaye, Iloka Chike Betram, Hope Uzoamaka Anyaragbu, Okorie Emeka Anthony, Omeye Emmanuel Chizoba, Okeke Ogochukwu Clementina

Department of Computer Science, Tansian University, Nigeria

Published November 2026

Abstract

Counterfeit and falsified medicines remain a significant public-health and pharmaceutical supply-chain challenge, particularly where consumers and frontline medicine users require rapid point-of-purchase verification. Existing technology-assisted approaches may depend on a single identifier, creating a potential point of compromise when an identifier is copied, reused or otherwise exposed. This study presents the design and implementation of a bi-modal drug authentication system that combines a machine-readable QR identifier with a concealed scratch authentication code. A design-science and experimental prototype approach was adopted. The system was implemented as a PHP/MySQL web application in an Apache/XAMPP development environment. Each authentication package is linked to a registered pharmaceutical product and contains a unique QR token and scratch code. During authentication, the QR token and scratch code are independently verified and their associated records are correlated before a final decision is produced. The prototype supports manufacturer and drug registration, authentication-package generation, QR-label printing, consumer authentication, transaction logging, suspicious-product monitoring and reused-code detection. Controlled tests covered valid pairs, invalid identifiers, mismatched identifiers, expired or revoked products and repeated authentication. Functional and integration testing showed that the implemented modules performed their specified operations, including successful detection and recording of invalid and reused authentication conditions. The study does not claim field-level accuracy or production response-time performance because independent repeated quantitative measurements were not available in the prototype evaluation. The contribution is therefore a technically demonstrated bi-modal authentication architecture that adds evidence correlation and traceability to consumer-level medicine verification and provides a basis for further field validation and regulatory integration.

Keywords: bi-modal authentication; drug authentication; QR code; scratch code; counterfeit medicines; pharmaceutical supply chain; Nigeria; evidence correlation; serialization

1 Introduction

1.1 Background

Medicines are essential to healthcare, but their safety depends not only on pharmacological quality but also on the integrity of the pharmaceutical supply chain. Procurement, storage, transportation, distribution and dispensing create multiple points at which medicine identity and integrity can be compromised. The World Health Organization (WHO, 2024) distinguishes substandard medicines, which fail to meet quality standards, from falsified medicines, which deliberately misrepresent their identity, composition or source. Such

products can contribute to treatment failure, adverse effects and other public-health consequences.

The problem is particularly relevant to low- and middle-income countries. Ozawa et al. (2018), in a systematic review and meta-analysis, estimated substantial prevalence of substandard and falsified medicines in low- and middle-income countries, with variation across medicine categories and settings. Evidence reviewed in the thesis also indicates continuing supply-chain challenges in Nigeria involving procurement, transportation, storage, financing, information management and other operational factors (Olutuase et al.,

2022). These conditions increase the importance of accessible mechanisms through which a consumer or authorised verifier can check a medicine against trusted records.

Nigeria has experience with consumer-level medicine authentication through the National Agency for Food and Drug Administration and Control (NAFDAC) Mobile Authentication Service (MAS), which uses concealed authentication codes and mobile communication. Previous studies have identified challenges associated with awareness, utilisation, network conditions and service reliability (Chinedu-Okeke et al.,

2021; Oyetunde et al., 2019). Other technological approaches include barcodes, QR codes, RFID, NFC, electronic track-and-trace systems, blockchain and cryptographic mechanisms (Rasheed et al., 2018; Zakari et al., 2022). The security of this consumer-facing process also depends on the protection of mobile devices and the personal information handled through them (Avwokuruaye, 2025).

QR codes are attractive for consumer-level verification because they can be scanned using ordinary smartphone cameras and can link a product to an online record. However, a QR code is not intrinsically proof of authenticity: a genuine code can potentially be copied and reproduced on another package. Scratch authentication codes introduce a concealed identifier and are already familiar within the Nigerian authentication context, but they may also face code-entry, service availability and reuse challenges. The central design proposition of this study is therefore to treat QR and scratch identifiers as complementary evidence sources rather than independent access channels. Both must correspond to the same authorised serialized product record before the system returns an authentic result.

1.2 Problem statement

Single-mode medicine authentication can create a single point of compromise. A QR-only system may validate a copied QR identifier if the copied identifier remains valid in the authentication database. A scratch-only system similarly depends on the secrecy and correct handling of the scratch credential. Conventional visual inspection can also be undermined by counterfeit packaging that reproduces legitimate

labels, registration details or other visible characteristics. Laboratory testing provides a different and stronger form of evidence about pharmaceutical composition, but it requires specialised equipment, expertise, time and resources and is not a routine point-of-purchase verification mechanism.

The research problem addressed in this study is therefore how to design a practical consumer-level authentication mechanism that reduces dependence on a single identifier, correlates two independent authentication credentials, detects mismatches and repeated use, and maintains an auditable history of authentication activity.

1.3 Aim and objectives

The aim of the study was to design and implement a bi-modal drug authentication system capable of verifying pharmaceutical products through two complementary authentication mechanisms.

The specific objectives were to:

- • examine existing drug-authentication methods and identify their limitations;
- • identify appropriate authentication modalities for pharmaceutical products;
- • design a bi-modal architecture for pharmaceutical authentication;
- • develop a database for storing and managing drug-authentication information;
- • implement the proposed bi-modal drug-authentication system;
- • evaluate the functional behaviour, reliability and technical performance of the prototype; and
- • compare the implemented approach conceptually with conventional single-mode authentication.

1.4 Contribution of the study

The principal contribution is an implemented web-based authentication prototype that links a QR token and concealed scratch code to the same authentication package. In addition to the consumer verification workflow, the system records authentication transactions and attempts, detects reused codes, records suspicious events and provides administrative monitoring. The study thus extends point-of-purchase authentication from a single identifier check toward evidence correlation and traceability.

2 Literature review

2.1 Counterfeit and falsified medicines

Counterfeit and falsified medicines are difficult to detect because they can be deliberately packaged to resemble genuine products. Kelesidis et al. (2013) identified substandard and counterfeit medicines as a significant global problem, while Ozawa et al. (2018) documented substantial prevalence and economic burden across low- and middle-income countries. More recent African evidence continues to show considerable country-level variation in the prevalence of substandard and falsified medicines (Mekonnen et al., 2024).

The Nigerian context adds supply-chain complexity. Olutuase et al. (2022) identified procurement, distribution, transportation, storage and information-management challenges in Nigerian medicine and vaccine supply chains. Authentication technology cannot resolve all of these structural problems, but it can provide an additional verification mechanism at the point where a product is being checked.

2.2 Existing authentication approaches

Traditional authentication involves visual inspection of packaging, manufacturer details, batch numbers, expiry dates and registration information. Although inexpensive, this approach depends on human judgement and can be defeated by sophisticated reproduction of genuine packaging (Institute of Medicine, 2013). Holograms and security labels provide additional physical features but can also be copied or damaged.

Scratch-code authentication provides a concealed credential that a consumer can reveal and submit through an authentication service. Nigerian research on MAS has identified operational and adoption challenges, including network and service problems and a gap between awareness and actual use (Chinedu-Okeke et al.,

2021; Oyetunde et al., 2019). Earlier work by Ukaoha et al. (2015) also demonstrated continued interest in mobile drug authentication for Nigerian users.

QR-based authentication enables smartphone scanning and rapid access to an online verification service. Tumenayu and Essien (2022) proposed an improved NAFDAC-oriented authentication approach using QR codes, illustrating the relevance of QR technology to the Nigerian environment. However, the copyability of a QR representation remains an important security consideration. RFID and NFC can support automated identification and supply-chain tracking, but they require additional infrastructure and compatible tags or readers. Blockchain has also been proposed for pharmaceutical traceability, although cost, interoperability, scalability and implementation complexity can be significant (Shetty et al., 2022; Zakari et al., 2022). More broadly, networked-device environments rely on reliable information exchange, interoperability and attention to privacy and security in connected systems (Olusanya et al., 2021).

2.3 Research gap

The reviewed literature indicates that several medicine-authentication approaches can improve consumer verification, but single identifiers remain vulnerable to copying, compromise or reuse. The specific gap addressed by this study is the integration of QR and scratch credentials as independent evidence sources tied to the same serialized product record, with a server-side correlation step before authentication. The design also incorporates authentication history and reused-code monitoring so that verification events can support subsequent administrative review.

3 Methodology

3.1 Research design

A design-science and experimental prototype approach was adopted. The design-science component focused on identifying the authentication problem, specifying system requirements, designing the architecture and database, implementing the software artefact, and evaluating its behaviour. The experimental component used controlled authentication scenarios to determine whether the prototype produced the expected result when valid, invalid, mismatched, expired, revoked or reused identifiers were presented.

The evaluation was technical rather than questionnaire-based. The thesis did not establish a field trial with a statistically representative consumer population, and the prototype's response-time section did not provide independent repeated benchmark measurements. Accordingly, the findings reported here are limited to the demonstrated functional and integration behaviour of the implemented system.

3.2 Data and test inputs

The study drew on scholarly literature, regulatory and pharmaceutical information, representative product records and controlled experimental authentication records. Where proprietary manufacturer data or confirmed counterfeit samples were unavailable, representative test records were used

for prototype evaluation. The controlled scenarios included valid QR plus matching scratch code; valid QR plus invalid scratch code; invalid QR; QR and scratch credentials belonging to different products; expired products; revoked products; and repeated use of an already authenticated code.

3.3 System architecture

The implemented architecture comprises an administrator layer, a consumer authentication interface, a PHP application layer, a MySQL database and a QR-code generation component. Administrators register manufacturers and drugs and generate authentication packages. Each package contains a unique authentication code, QR token, QR payload and scratch code. The QR token is embedded in a URL so that scanning the printed QR code opens the consumer authentication page and automatically supplies the QR token. The consumer then enters the concealed scratch code.

The server independently verifies the QR token and scratch code, retrieves the corresponding product records, compares their association, checks product and credential status, evaluates prior use and then generates the final authentication result. Authentication transactions and attempts are recorded for administrative monitoring.

3.4 Authentication decision logic

The decision mechanism is rule-based. An authentication request is accepted as authentic only when the QR token is registered, the scratch code is registered, both identifiers belong to the same active product package, the product is not expired or revoked, and the credential has not already been used in a manner prohibited by

the system rules. Invalid or mismatched credentials are not treated as authentic. This makes the evidence- correlation step central to the system rather than simply providing two alternative ways of accessing the same

database.

Table 1. Authentication decision rules and system outcomes.

QR result	Scratch result	Relationship/status	System decision
Valid	Correct	Same active, unused package	AUTHENTIC
Valid	Invalid	Active product	INVALID SCRATCH CODE / suspicious condition
Invalid	Any	Unregistered QR	INVALID QR / not authenticated
Valid	Correct	Expired product	EXPIRED
Valid	Correct	Revoked/inactive product	REVOKED / not authenticated
Valid	Correct	Previously authenticated	REUSED CODE
Valid	Correct	Different product	SUSPICIOUS
Invalid	Invalid	No authorised match	NOT AUTHENTICATED

3.5 Implementation technologies

The prototype was implemented as a web application using PHP for server-side processing and MySQL for relational data storage. Apache/XAMPP was used as the development and test environment. The interface used HTML5, CSS3, JavaScript and Bootstrap 5.3.3. PHP Data Objects (PDO) was used for database access, while a QR-code library was used to generate printable QR labels. The design also incorporated password hashing, secure random generation of authentication credentials, database uniqueness constraints, prepared queries and session-based administrator access control.

3.6 Database design

The database contains tables for administrators, manufacturers, drugs, authentication codes, authentication transactions, authentication attempts, consumer authentication logs and suspicious products. The authentication_codes table stores the paired QR token and scratch code and links them to a registered drug. Unique constraints are applied to relevant identifiers. Authentication transactions preserve verification results and timestamps, while attempt and suspicious-product records support traceability and administrative investigation.

4 Results

4.1 Implemented system functions

The implemented prototype provides an end-to-end workflow from product registration to consumer verification and administrative monitoring. Administrators can register manufacturers and drugs, generate authentication packages, manage QR labels and review authentication activity. Consumers can scan a QR code, arrive at the authentication page with the QR token supplied by the URL and enter the concealed scratch code.

Table 2. Implemented system functions and prototype outcomes.

Function	Expected behaviour	Prototype outcome
Administrator login	Valid credentials provide dashboard access	Pass
Manufacturer registration	Unique manufacturer record is stored	Pass
Drug registration	Valid product and batch record is stored	Pass
Authentication package generation	Unique QR and scratch credentials are generated	Pass
QR-code printing	QR token is converted into printable label	Pass
Consumer authentication	QR scan plus scratch code produces decision	Pass
Authentication logging	Every attempt is recorded	Pass
Suspicious/reuse monitoring	Invalid/reused conditions are available for review	Pass
Statistics	Authentication counts are available to administrator	Pass

4.2 Integration and security testing

Integration testing confirmed the major relationships among manufacturer records, drugs, authentication packages, QR-token retrieval, scratch-code validation, transaction insertion, attempt logging and suspicious- product recording. A critical integration condition was that the product returned through QR verification had to be the same product associated with the scratch credential. This prevented two individually valid identifiers belonging to different products from being accepted as an authentic pair.

Security-oriented tests included invalid administrator login, access to protected administrator pages, SQL- injection input handling, duplicate QR-token and scratch-code attempts, scratch-code guessing and repeated use of an authenticated package. The implementation used prepared statements, session protection, password hashing, random credential generation, database uniqueness constraints and use-count monitoring. These controls provide application-level safeguards but do not by themselves constitute a complete production security assessment.

4.3 Controlled experimental scenarios

Table 3. Controlled experimental authentication scenarios and expected decisions.

Scenario	QR	Scratch	Product/code state	Expected decision
E01	Valid	Correct	Active and unused	AUTHENTIC
E02	Valid	Incorrect	Active	INVALID SCRATCH CODE
E03	Invalid	Any	Unregistered QR	INVALID QR
E04	Valid	Correct	Expired drug	EXPIRED
E05	Valid	Correct	Revoked/inactive drug	REVOKED
E06	Valid	Correct	Previously authenticated	REUSED CODE
E07	Valid	Correct	Active and unused	AUTHENTIC
E08	Valid	Incorrect	Active	INVALID SCRATCH CODE
E09	Invalid	Any	Unregistered QR	INVALID QR
E10	Valid	Correct	Active and unused	AUTHENTIC

The controlled scenarios demonstrate the principal functional capability of the prototype: authentication is based on the relationship between two credentials and the status of the product, rather than on the validity of a single identifier alone. In particular, a valid QR code does not produce an authentic decision when the scratch credential is invalid, reused or associated with a different product.

4.4 Comparative interpretation

Table 4. Conceptual comparison of single-mode and bi-modal authentication.

Dimension	Single-mode authentication	Implemented bi-modal approach
Authentication evidence	One identifier	QR token plus concealed scratch code

Dimension	Single-mode authentication	Implemented bi-modal approach
Copied QR exposure	Copied identifier may remain usable	Copied QR alone cannot complete authentication
Reuse monitoring	Depends on implementation	Use-count and reused-code monitoring included
Traceability	May record one verification event	Transactions, attempts and suspicious records maintained
Consumer workflow	One verification input	QR scan followed by scratch-code entry
Administrative monitoring	Varies by system	Attempts, suspicious products, reused codes and statistics

The comparison is conceptual rather than a statistical head-to-head benchmark. The prototype introduces a second authentication condition, so a copied QR identifier alone is insufficient when the corresponding scratch credential is absent, invalid or inconsistent. This is the primary security consequence of the proposed evidence-correlation model.

4.5 Performance evaluation boundary

The prototype supports response-time measurement, but the thesis did not supply independently measured repeated response-time values suitable for reporting as production performance. It would therefore be methodologically inappropriate to insert illustrative milliseconds, accuracy percentages, false-acceptance rates or false-rejection rates into this article as if they were empirical field findings. Future evaluation should measure QR lookup, scratch verification and complete authentication over repeated trials under defined server, database, network and device conditions.

5 Discussion

The study demonstrates the feasibility of combining two familiar consumer authentication mechanisms within one web-based system. The design responds directly to a weakness identified in the reviewed literature: reliance on a single authentication identifier. QR codes are convenient because they provide a smartphone-accessible entry point, but their visual representation can be reproduced. Scratch codes introduce a concealed credential and are consistent with the authentication principle used by Nigeria's MAS. The implemented system does not simply offer both mechanisms independently; it requires their results to correspond to the same authorised product record.

This evidence-correlation approach is important because independent validity is not sufficient. For example, a QR token from Product A and a scratch code from Product B could each be valid in the database while still representing an invalid combination. The correlation rule identifies this inconsistency and prevents the combination from being classified as authentic. The approach therefore adds an explicit relationship check that is absent from a single-identifier verification process.

The implementation also extends point-of-purchase verification into an administrative monitoring function. Authentication transactions, attempts and suspicious-product records provide a history that can be reviewed after individual verification events. Reused codes are tracked through use_count and exposed through administrative monitoring. These features are relevant because a counterfeit or compromised identifier may generate patterns that become more informative when repeated authentication events are retained.

The findings should nevertheless be interpreted within the limits of a prototype study. The system was evaluated in a controlled development environment rather than through a national pharmaceutical deployment. Network availability, server hardening, database scale, manufacturer integration, consumer usability and regulatory interoperability require further evaluation. In addition, digital authentication establishes correspondence with trusted records; it does not establish chemical composition, potency, purity or contamination. Laboratory quality testing therefore remains a distinct requirement.

6 Practical and research implications

For pharmaceutical manufacturers and authorised distributors, the architecture demonstrates how

serialization can support package-level identifiers and post-market authentication records. For consumers and pharmacists, the QR-plus-scratch workflow provides a straightforward sequence that uses a smartphone camera and one manually entered credential. For regulators and system operators, the transaction, attempt

and suspicious-event records provide a foundation for monitoring and investigation. These implications are technological and operational; the prototype should not be interpreted as a replacement for NAFDAC regulatory processes.

For researchers, the system provides a basis for future work on stronger cryptographic protection, offline or intermittent-connectivity authentication, privacy-preserving audit trails, secure manufacturer integration, large-scale performance evaluation, user acceptance studies and controlled field trials involving authorised pharmaceutical products.

7 Limitations

First, the prototype was evaluated using controlled scenarios rather than a nationally representative sample of pharmaceutical products. Second, confirmed counterfeit samples may be difficult to obtain because of safety, legal and ethical constraints; simulated conditions were therefore necessary for some test cases. Third, the prototype depends on a functioning web server, database and network connection. Fourth, detailed manufacturer data may be restricted by proprietary considerations. Fifth, the study did not provide measured field-level accuracy, false-acceptance, false-rejection or production response-time statistics. Finally, the prototype does not replace laboratory testing or regulatory inspection.

8 Conclusion

This study designed and implemented a bi-modal drug authentication system that combines QR-code verification with concealed scratch-code verification for pharmaceutical products. The prototype

demonstrates an end-to-end workflow in which each authentication package is linked to a registered product and the two identifiers are independently checked and correlated before a final decision is returned. The implemented system also provides transaction logging, authentication-attempt history, suspicious-product recording, reused-code monitoring and administrative statistics.

The principal technical contribution is the use of evidence correlation to reduce dependence on a single identifier. A copied QR code alone is not sufficient for an authentic result when the corresponding scratch code is absent, invalid, reused or associated with another product. The

prototype therefore provides a practical additional layer for medicine verification in the Nigerian context. However, the results establish technical feasibility rather than nationwide effectiveness. Before deployment, the system requires security hardening, HTTPS/TLS, stronger secret management, formal backup and recovery procedures, larger-scale performance testing, authorised field validation and consideration of integration with relevant regulatory processes.

9 Recommendations

- • Retain the two-identifier model so that a copied QR label alone cannot complete authentication.
- • Generate cryptographically strong and unique QR tokens and scratch codes for individual serialized packages.
- • Enforce database uniqueness constraints and monitor authentication-code reuse.
- • Maintain transaction, attempt and suspicious-event records to support traceability and investigation.
- • Deploy the application over HTTPS/TLS with hardened hosting, secure secret management and tested backup and recovery procedures.
- • Conduct controlled field validation using authorised pharmaceutical products and appropriate regulatory oversight.
- • Undertake user-acceptance research to assess usability, comprehension of authentication results and adoption barriers.
- • Evaluate integration with relevant Nigerian regulatory and pharmaceutical supply-chain systems where
- formally authorised.

References

[1] Academies Press. https://doi.org/10.17226/18272

[2] Avwokuruaye, O. (2025). Securing personal data in the smartphone age: A study of mobile device security. *International Journal of Science Research and Technology*, 9(9), 155–172. https://doi.org/10.70382/tijsrat.v09i9.050

[3] Chinedu-Okeke, C. F., Okoro, N., & Obi, I. (2021). Mobile Authentication Service (MAS) scheme and public participation in eradicating fake drugs in South-East Nigeria. *International Journal of Research and Innovation in Social Science*, 5(6), 90–98. https://doi.org/10.47772/IJRISS.2021.5605

[4] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. https://doi.org/10.2307/249008

[5] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

[6] Institute of Medicine. (2013). Countering the problem of falsified and substandard drugs. *The National*

[7] Kelesidis, T., Kelesidis, I., Rafailidis, P. I., & Falagas, M. E. (2013). Substandard and counterfeit medicines: A systematic review of the literature. *BMJ Open*, 3(8), e002923. https://doi.org/10.1136/bmjopen-2013- 002923

[8] Mekonnen, B. A., Yizengaw, M. G., & Worku, M. C. (2024). Prevalence of substandard, falsified, unlicensed and unregistered medicine and its associated factors in Africa: A systematic review. *Journal of Pharmaceutical Policy and Practice*, 17(1), 2375267. https://doi.org/10.1080/20523211.2024.2375267

[9] Mengesha, A., Bastiaens, H., Ravinetto, R., Gibson, L., & Dingwall, R. (2024). Substandard and falsified medicines in African pharmaceutical markets: A case study from Ethiopia. *Social Science & Medicine*, 349, 116882. https://doi.org/10.1016/j.socscimed.2024.116882

[10] Olusanya, G. S., Okunbor, C., & Avwokuruaye, O. (2021). Internet of Things (IoT) as the future of networked devices: An overview. *Global Journal of Engineering and Technology Advances*, 9(3), 031–037. https://doi.org/10.30574/gjeta.2021.9.3.0154

[11] Olutuase, V. O., Iwu-Jaja, C. J., Akuoko, C. P., Adewuyi, E. O., & Khanal, V. (2022). Medicines and vaccines supply chains challenges in Nigeria: A scoping review. *BMC Public Health*, 22, 11. https://doi.org/10.1186/s12889-021-12361-9

[12] Oyetunde, O. O., Ogidan, O., Akinyemi, M. I., Ogunbameru, A. A., & Asaolu, O. F. (2019). Mobile authentication service in Nigeria: An assessment of community pharmacists' acceptance and providers' views of successes and challenges of deployment. *Pharmacy Practice*, 17(2), 1449. https://doi.org/10.18549/PharmPract.2019.2.1449

[13] Ozawa, S., Evans, D. R., Bessias, S., Haynie, D. G., Yemeke, T. T., Laing, S. K., Herrington, J. E., & Preker, A. S. (2018). Prevalence and estimated economic burden of substandard and falsified medicines in low- and middle-income countries: A systematic review and meta-analysis. *JAMA Network Open*, 1(4), e181662. https://doi.org/10.1001/jamanetworkopen.2018.1662

[14] Protected QR code-based anti-counterfeit system for pharmaceutical manufacturing. (2026). Procedia CIRP, 138, 322–327. https://doi.org/10.1016/j.procir.2026.01.056

[15] Rasheed, H., Höllein, L., & Holzgrabe, U. (2018). Future information technology tools for fighting substandard and falsified medicines in low- and middle-income countries. *Frontiers in Pharmacology*, 9, 995. https://doi.org/10.3389/fphar.2018.00995

[16] Shetty, A. D., Shenoy, S. S., Sreedhar, D., Shetty, A., Rao, R., & Dsouza, K. J. (2022). Traceability of counterfeit drugs in pharma supply chain through blockchain technology: A systematic review of the evidence. *Research Journal of Pharmacy and Technology*, 15(2), 908–912. https://doi.org/10.52711/0974-360X.2022.00152

[17] Sorato, M. M., Davari, M., & Kebriaeezadeh, A. (2024). Improving access to medicines to reduce marketing and use of substandard and falsified medicines in Africa: Scoping review. *Journal of Pharmaceutical Policy and Practice*, 17, 27550834241236598. https://doi.org/10.1177/27550834241236598

[18] Tumenayu, O. O., & Essien, U. E. (2022). Design and implementation of an improved NAFDAC Mobile Authentication Services using Quick Response Code. *Unicross Journal of Science and Technology*, 1(1), 30–38.

[19] Ukaoha, K. C., Dim, C. N., Daodu, S. S., & Odikayor-Ogbomo, F. I. (2015). Towards a mobile drugs authentication system for Nigerian users. *Computing*, Information Systems, Development Informatics & Allied Research Journal, 6(1), 35–40.

[20] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

[21] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. https://doi.org/10.2307/30036540

[22] World Health Organization. (2024, December 3). *Substandard and falsified medical products*. https://www.who.int/en/news-room/fact-sheets/detail/substandard-and-falsified-medical-products

[23] Zakari, N., Al-Razgan, M., Alsaadi, A., Alshareef, H., Al Saigh, H., Alashaikh, L., Alharbi, M., Alomar, R., & Alotaibi, S. (2022). Blockchain technology in the pharmaceutical industry: A systematic review. *PeerJ Computer Science*, 8, e840. https://doi.org/10.7717/peerj-cs.840