InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-2 / February - 2026

Original Article

A Threat-Aware and Explainable ML framework coordinated by Block chain for counterfeit drug detection

Muskan Devnani
Pooja Shere Carol Chettiar

Manuscript ID:
IBMIIRJ -2026-030208

Submitted: 06 Jan. 2026

Revised: 10 Jan. 2026

Accepted: 04 Feb. 2026

Published: 28 Feb. 2026

ISSN: 3065-7857

Volume-3

Issue-2

Pp. 40-43

February 2026

Correspondence Address:
Muskan Devnani,
Pooja Shere Carol Chettiar

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.21131488

DOI Link:
https://doi.org/10.5281/zenodo.21131488

Abstract

Counterfeit drugs pose a serious threat to public health and pharmaceutical supply chain integrity. Existing approaches primarily rely on either machine learning for counterfeit detection or blockchain based traceability systems, but they fail to address evolving counterfeit strategies and lack ransparency in decision making. This research proposes a threat aware and explainable machine learning framework coordinated by blockchain to detect counterfeit drugs in real time. The proposed system simulates potential adversarial counterfeit behaviors to train a robust ML model capable of detecting unseen attacks. Additionally, explainable AI techniques are employed to provide clear reasoning behind each authenticity decision, increasing regulatory acceptance. Blockchain is used as a trusted coordination layer to store immutable supply-chain data, verify ML outputs, and secure explanation proofs using smart contracts. The proposed framework enhances detection accuracy, transparency, and resilience against future counterfeit threats.

Keywords: *Counterfeit Drug Detection, Threat-Aware Machine Learning, Explainable Artificial Intelligence (XAI), Blockchain-Based Supply Chain, Adversarial Learning, Pharmaceutical Supply Chain Security, Smart Contracts, Transparency and Trust, Zero-Day Attack Detection*

Introduction

Counterfeit pharmaceutical drugs have emerged as a severe global concern, causing significant health risks, economic losses, and erosion of trust in healthcare systems. According to international health organizations, counterfeit medicines account for a substantial portion of drugs in circulation, particularly in developing regions. These counterfeit products often bypass traditional supply-chain verification mechanisms due to sophisticated forgery techniques and data manipulation strategies.Recent advancements in machine learning have enabled automated counterfeit detection using packaging images, QR codes, and transactional data. However, most existing systems are reactive in nature, trained solely on historical counterfeit patterns. Such models fail when attackers adopt new strategies that deviate known patterns. Additionally, these machine learning systems often function as black boxes, providing no explanation for their decisions, which limits their adoption in regulatory and legal contexts. Blockchain technology has been proposed as a solution for improving supply-chain transparency and traceability. While blockchain enhances data integrity, it does not provide intelligence for detecting counterfeit behavior, nor does it verify the reasoning behind AI-based alerts. To address these limitations, this paper proposes a novel framework that integrates threat-aware machine learning, explainable artificial intelligence, and blockchain coordination to detect counterfeit drugs in transparent, robust and future-ready manner.

Related Work

Several studies have explored machine learning techniques for counterfeit drug detection using image Analysis, QR code verification and supply-chain monitoring. Traditional classifiers and deep learning Models have demonstrated effectiveness in detecting known counterfeit patterns. However, these approaches are limited by their dependency on static datasets and inability to generalize against evolving threats. Explainable AI techniques have gained attention in healthcare and financial domains to improve transparency and trust in automated systems. Nevertheless, their application in pharmaceutical counterfeit detection remains limited and fragmented. Blockchain-based solutions have been widely adopted for supply-chain traceability, ensuring immutable record-keeping and improved transparency.

How to cite this article:
Devnani, M. (2026). A Threat-Aware and Explainable ML framework coordinated by Block chain for counterfeit drug detection. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(2), 40–43. https://doi.org/10.5281/zenodo.21131488

However, most blockchain implementations focus solely on data storage and verification, without integrating intelligent threat detection or explanation mechanisms. Existing literature largely treats machine learning, explainability, and blockchain as independent solutions. There is a notable of a unified framework that combines threat-aware learning with explainable decision-making and blockchain-based trust coordination in the context of counterfeit drug detection.

Research Gap and Motivation

1. Despite significant progress in counterfeit detection technologies, the following gaps remain:
2. Lack of proactive detection mechanisms capable of identifying unseen and evolving counterfeit strategies.
3. Absence of explainable decision-making in existing machine learning-based systems.
4. Limited use of blockchain beyond basic data traceability.
5. No framework that verifies and audits AI explanations using decentralized trust mechanisms.
   This research is motivated by the need to develop a holistic system that is resilient to adaptive threats, transparent in its decision-making and trusted by regulatory authorities.

Proposed Framework Overview

The proposed framework consists of three core layers;

1. Threat-aware machine learning layer
2. Explainable AI layer
3. Blockchain coordination layer

These layer work collaboratively to detect counterfeit drugs, explain detection decisions, and ensure trust and auditability.

1. **Threat-aware machine learning layer**

Traditional machine learning models assume that counterfeit patterns remain static. In contrast, the proposed framework incorporates Adversarial

Learning to simulate potential future counterfeit strategies. Adversarial samples are generated to represent:

- QR code cloning and partial tampering
- Minor packaging and hologram alterations
- Supply-chain route deviations
- Delayed or missing transaction updates

The model is trained on a combination of genuine pharmaceutical data and adversarially generated counterfeit samples. This enables the learning of generalized counterfeit indicators rather than memorization of historical patterns, improving robustness against zero-day counterfeit attacks.

2. **Explainable AI layer**

To ensure transparency and regulatory compliance, the Explainable AI layer interprets the decisions made by the machine learning model.

Instead of binary outputs, the system identifies contributing factors responsible for classification outcomes.

Explanations are generated across multiple dimensions:

- Visual inconsistencies in packaging
- Anomalies in supply-chain routes
- Temporal mismatches in transaction logging

Each factor is assigned a contribution weight, allowing stakeholders to understand why a particular drug was flagged as counterfeit.

This improves trust, accountability and legal defensibility.

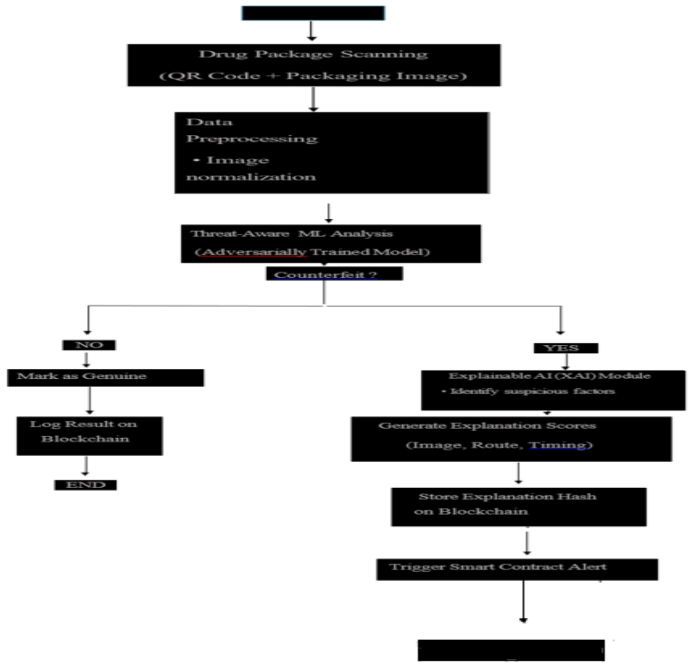
3. **Bloc0kchain coordination layer**

   Blockchain functions as a decentralized trust layer coordinating interactions between supply-chain participants and the AI system. Its responsibilities include:

- Immutable logging of supply-chain events
- Verification of QR code scans and timestamps
- Storage of cryptographic hashes of AI explanations
- Automated alert triggering using smart contracts

By storing hashed proofs of explanations rather than raw data, the system ensures data privacy while maintaining auditability and non-repudiation.

System Architecture



The system architecture follows a modular layered design. Drug packaging data is collected through QR code scanning and image capture.Supply-chain transaction data is retrieved from the blockchain ledger. The threat-aware ML engine analyses combined data, after which the XAI module generates interpretable explanations. Blockchain smart contracts verify explanation integrity and trigger alerts when counterfeit probability exceeds predefined thresholds.

Experimental Setup Dataset Description

Due to limited access to real-world counterfeit datasets, a hybrid dataset is
Constructed consisting of:

- Genuine pharmaceutical packaging images
- Synthetic counterfeit samples generated using adversarial techniques
- Simulated supply-chain transaction records

This approach reflects realistic attack scenarios and supports evaluation of robustness against unseen threats.

Evaluation Metrics

The proposed framework is evaluated using:

- Accuracy
- Precision
- Recall
- F1-score
- Adversarial robustness
- Explanation consistency

Results and Discussion

Experimental results indicate that the threat-aware model outperforms conventional machine learning models when exposed to unseen counterfeit strategies. The inclusion of adversarial training significantly improves recall without compromising precision. Explainable. AI outputs enhance interpretability, while blockchain coordination ensures data and explanation integrity.

Conclusion and Future Work

This paper presents a novel Threat-Aware and Explainable Machine Learning framework coordinated by Blockchain for counterfeit drug detection. By integrating adversarial learning, explainable decision-making, and decentralized trust, the proposed system addresses critical limitations of existing approaches. Future work includes real-world deployment, integration with IoT-based sensors, and evaluation using large-scale pharmaceutical datasets.

Acknowledgment

The authors would like to express their sincere gratitude to all those who contributed, directly or indirectly, to the successful completion of this research work. We are thankful to our institution for providing the necessary academic environment, resources, and support required for this study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Goodfellow, I., et al., "Explaining and Harnessing Adversarial Examples," ICLR, 2015. https://arxiv.org/abs/1412.6572
2. Ribeiro, M. T., et al., "Why Should I Trust You?," KDD, 2016.
3. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.
4. https://dl.acm.org/doi/abs/10.1145/2939672.2939778
5. Biggio, B., & Roli, F.
6. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. Pattern Recognition, Elsevier, vol. 84, pp. 317–331, 2018.
7. https://dl.acm.org/doi/abs/10.1145/3243734.3264418
8. Lundberg, S. M., & Lee, S.-I.
9. A Unified Approach to Interpreting Model Predictions.
10. Advances in Neural Information Processing Systems (NeurIPS), 2017
11. https://proceedings.neurips.cc/paper/2017/hash/ 8a20a8621978632d76c43dfd28b67767-Abstract.html
12. Doshi-Velez, F., & Kim, B. Towards a Rigorous Science of Interpretable Machine Learning. arXiv preprint arXiv:1702.08608, 2017. https://arxiv.org/abs/1702.08608
13. Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. Governance on the Drug Supply Chain via Blockchain Technology. Journal of Food and Drug Analysis, vol. 26, no. 3, pp. 938–946, 2018. https://www.mdpi.com/1660-4601/15/6/1055
14. Mackey, T. K., & Nayyar, G. A Review of Existing and Emerging Digital Technologies to Combat the Global Trade in Fake Medicines. Expert Opinion on Drug Safety, vol. 16, no. 5, pp. 587–602, 2017. https://www.tandfonline.com/doi/abs/ 10.1080/14740338.2017.1313227
15. Esteva, A., et al. A Guide to Deep Learning in Healthcare. Nature Medicine, vol. 25, pp. 24–29, 2019. https://www.nature.com/articles/s41591-018-0316-z
16. Gunning, D. Explainable Artificial Intelligence (XAI).
17. DARPA, 2017.
18. https://www.darpa.mil/sites/default/files/attachment/2025-02/darpa- program-xai-industry-day-presentation.pdf