
Blockchain-Integrated and Privacy-Preserving AI Framework for Drug Authenticity Verification in Intelligent Pharmaceutical Supply Chains

Shamali A. Gupte¹ and Rajkumar Shende²

^{1,2}*Department of Computer Engineering, St. Francis Institute of Technology (SFIT),
Mumbai, India*

¹*shamaligupte@student.sfit.ac.in*, ²*rajkumarshende@sfit.ac.in*

Abstract.

Fake medications pose serious risks to patient safety and healthcare trust, particularly in developing nations. Conventional authentication methods can verify product identifiers but remain vulnerable to duplication. This paper introduces DAVASC, a decentralized authenticity verification architecture integrating permissioned Hyperledger Fabric, a GAT-Transformer model, and Secure Multi-Party Computation (SMPC). A Merkle-DAG mechanism securely anchors transaction records across permissioned and public ledgers while supporting regulatory audits. Evaluated on 120,000 synthetic pharmaceutical transactions covering six counterfeit injection methods, DAVASC achieves 97.4% centralized and 96.8% SMPC-based detection accuracy, 68.3 TPS throughput, and confirmation times below 12 milliseconds, demonstrating secure, scalable, and reliable counterfeit detection.

Keywords: Pharmaceutical Supply Chain Security; Drug Authenticity Verification; Hyperledger Fabric; Graph Attention Network; Secure Multi-Party Computation; Merkle-DAG.

1. INTRODUCTION

The global pharmaceutical market reached an estimated value of USD 1.48 trillion in 2022, yet a substantial share of medicines in developing nations still fail to meet quality and authenticity standards. The World Health Organization (WHO) estimates that about 10% of medicines worldwide are substandard or falsified [1]. The 2009 heparin contamination incident, which caused nearly 250 fatalities in the United States, and the ongoing theft of antimalarial drugs across sub-Saharan Africa illustrate how supply chain failures translate directly into clinical harm. The US Drug Supply Chain Security Act (DSCSA), the EU Falsified Medicines Directive (FMD), and WHO prequalification programs have introduced stronger traceability requirements, but markets most prone to counterfeiting still lack the infrastructure to comply with them. Prior work has explored IoT-based cold-chain monitoring, cross-border consortium traceability, zero-knowledge price attestation, and univariate anomaly detection on transaction logs, but none of these approaches combine relational graph modeling with SMPC-level privacy.

Blockchain technology provides a shared, protected ledger that multiple parties can access to record custody activity with permanent integrity. Smart contracts extend this by automating enforcement actions without relying on a centralized authority. This study applies graph-based deep learning to identify genuine anomalies within high-volume transaction streams. By combining a permissioned Hyperledger Fabric ledger with a GAT-T detection model trained under SMPC, DAVASC delivers regulatory-grade auditability, commercial confidentiality, and real-time counterfeit detection.

1.1. *Principal Contributions*

The principal contributions of this work are as follows: DAVASC integrates Hyperledger Fabric, privacy-preserving GAT-T detection, Merkle-DAG anchoring, and SMPC training to secure pharmaceutical supply chains, achieving 97.4% accuracy, 96.8% SMPC accuracy, and 68.3 TPS.

2. RELATED WORK

Blockchain adoption in pharmaceutical supply chains has largely focused on traceability rather than behavioral intelligence. Uddin [6] developed permissioned Hyperledger Fabric ledger designs for drug traceability, and Bandhu et al. [7] demonstrated smart contract-based recall mechanisms, but neither incorporated a fraud detection layer. Singh et al. [2] addressed IoT-based cold-chain monitoring, and Musamih et al. [3] addressed cross-border drug traceability, while Uddin et al. [4] introduced blockchain architectures with zero-knowledge attestation, a confidentiality mechanism that DAVASC extends through SMPC. On the machine learning side, Alqarni et al. [5] explored smart contract automation in supply chains; Wang et al. [8] showed that graph convolutional networks are effective fraud detectors in relational transaction data; Naga Sudha and Nayahi [9] showed that Hyperledger-based temporal supply chain modeling captures multi-transaction patterns; and Padma and Ramaiah [10] examined secure information sharing in pharmaceutical supply chains using blockchain and smart contracts. No prior system combines graph-structured relational modeling, SMPC-level privacy, cross-chain auditability, and automated enforcement in a single framework.

3. PROPOSED DAVASC FRAMEWORK

3.1. *Hyperledger Fabric Design with Merkle-DAG Anchoring*

DAVASC runs on Hyperledger Fabric version 2.5 with four ordering-service nodes operating under Raft consensus and eight peer nodes distributed across manufacturer, distributor, wholesaler, and pharmacy organizations. The Merkle-DAG anchoring mechanism works as follows. Every $\Delta_t = 500$ transactions, the DAVASC anchor service computes a Merkle root M_n from the transaction hashes in the current batch interval:

$$M_n = \text{MerkleRoot}(H(tx_i) : i \in [n \cdot \Delta_t, (n + 1) \cdot \Delta_t]) \quad (1)$$

3.2. *GAT-T Anomaly Detection Model*

The Graph Attention Network component of GAT-T computes, for each transaction edge $e = (u, v, t)$, a learned representation of how structurally unusual that transaction is relative to

its local network context. For node u with neighbor set $N(u)$, the attention coefficient α_{ij} is defined as:

$$\alpha_{ij} = \text{softmax}_i(\text{LeakyReLU}(a^T \cdot [W h_i || W h_j])) \quad (2)$$

GAT uses multi-head attention to model relationships within the supply chain. The LSTM-enhanced Transformer, on the other hand, is used for analyzing transaction sequences and recognizing counterfeit activity patterns:

$$A(e) = \sigma(W_2 \cdot \text{ReLU}(W_1 \cdot [z_{\text{GAT}} || z_{\text{Trans}}] + b_1) + b_2) \quad (3)$$

When $A(e)$ exceeds the threshold $\tau = 0.78$, the smart contract freezes the affected batch, raises a tamper-evident alert on the public chain, and sends HTTPS notifications to the relevant regulatory authority and all downstream holders of the asset.

3.3. SMPC Training Protocol

DAVASC trains the GAT-T model using SPDZ, a multi-party computation protocol that provides strong cryptographic security against a dishonest majority of participants under a semi-honest threat model. Each stakeholder node i holds a secret share $[w]_i$ of the global model weight vector w .

$$\Pi_{\text{SMPC}} : \forall i, j \in [K], i \neq j : I([w]_i, D_j) = 0 \quad (4)$$

This expression states that the mutual information between node i 's model share and node j 's dataset is zero: observing node i 's share reveals nothing about node j 's data.

4. EXPERIMENTAL METHODOLOGY

4.1. Dataset

DAVASC was evaluated on a synthetic dataset of 120,000 pharmaceutical transactions generated across 12 WHO-modeled supply chain topologies spanning January 2020 to December 2023. Each record includes a batch identifier, drug classification, custody parties, timestamp, geolocation hash, price deviation, temperature flag, and certification status. Six counterfeit strategies (serial cloning, price undercutting, routing bypass, certification reuse, temperature falsification, and multi-hop laundering) were embedded at an overall prevalence of 9.1%, with the data split 70/15/15 for training, validation, and testing.

4.2. Baselines and Evaluation Metrics

Five baseline models were compared against the proposed GAT-T architecture: Isolation Forest, Random Forest, a Support Vector Machine with an RBF kernel, a standalone Graph Convolutional Network (GCN), and a standalone Transformer. All models were evaluated on Accuracy, Precision, Recall, and F1-Score using a held-out test set of 18,000 samples at 9.1% counterfeit prevalence. Blockchain performance was benchmarked against a standard Hyperledger Fabric (v2.5) baseline and a Hyperledger Besu private chain.

5. RESULTS AND DISCUSSION

5.1. Machine Learning Model Performance

Table 1 shows GAT-T achieving the highest performance, with 97.4% accuracy and 97.1% F1-score. SMPC training achieves 96.8% accuracy, demonstrating minimal privacy-related performance loss.

Table 1. Classification performance comparison across ML models on the test set.

ML Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Isolation Forest	88.4	87.9	86.1	87.0
Random Forest	90.7	89.2	91.1	90.1
SVM (RBF Kernel)	87.2	85.8	84.6	85.2
Standalone GCN	93.1	92.5	91.8	92.1
Standalone Transformer	92.7	91.3	92.9	92.1
GAT-T Centralized	97.4	96.9	97.3	97.1
GAT-T SMPC (Proposed)	96.8	96.2	96.7	96.4

5.2. Blockchain and System Performance

Table 2 reports blockchain performance metrics for DAVASC against a standard Hyperledger Fabric baseline and a Hyperledger Besu private chain configuration comparable to those used in prior pharmaceutical traceability work.

Table 2. DAVASC vs. Hyperledger Fabric baseline and Hyperledger Besu.

Metric	H. Fabric Baseline	H. Besu Private	DAVASC (Proposed)	Unit
Throughput	40-50	35-45	68.3	TPS
Avg. Block Latency	~500	~800	< 12	ms
Smart Contract Exec.	~320	~450	~140	ms
Energy/Transaction	~0.008	~0.012	~0.003	J
Privacy Mechanism	Channel isolation	None	SMPC + Merkle-DAG	—
Cross-chain Audit	No	No	Yes (Ethereum anchor)	—
Attack Resistance	Partial	Partial	Full (4 vectors)	—

6. CONCLUSION AND FUTURE WORK

This paper introduced DAVASC, a decentralized framework combining Hyperledger Fabric, GAT-Transformer anomaly detection, SMPC-based privacy, and Merkle-DAG anchoring for pharmaceutical supply-chain security. The system achieved 97.4% centralized accuracy, 97.1% F1-score, and 96.8% accuracy under SMPC, with only 0.6 percentage-point privacy loss. Hyperledger Fabric delivered 68.3 TPS with sub-12 ms latency, while attack detection ranged from 87% to 99.2%. Future work includes hospital-pharmacy deployment, asynchronous SMPC, and GDPR-compliant chaincode.

7. REFERENCES

- [1] World Health Organization, "Substandard and falsified medical products," WHO Fact Sheet, 2023. <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>.
- [2] R. Singh, A. D. Dwivedi, and G. Srivastava, "Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," *Sensors*, vol. 20, no. 14, p. 3951, 2020. <https://doi.org/10.3390/s20143951>.
- [3] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE Access*, vol. 9, pp. 9728–9743, 2021. <https://doi.org/10.1109/ACCESS.2021.3049920>.
- [4] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, "Blockchain for drug traceability: Architectures and open challenges," *Health Informatics Journal*, vol. 27, no. 2, p. 14604582211011228, 2021. <https://doi.org/10.1177/14604582211011228>.
- [5] M. A. Alqarni, M. S. Alkatheiri, S. H. Chauhdary, and S. Saleem, "Use of blockchain-based smart contracts in logistics and supply chains," *Electronics*, vol. 12, no. 6, p. 1340, 2023. <https://doi.org/10.3390/electronics12061340>.
- [6] M. Uddin, "Blockchain Medledger: Hyperledger Fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, p. 120235, 2021. <https://doi.org/10.1016/j.ijpharm.2021.120235>.
- [7] K. C. Bandhu, R. Litoriya, P. Lowanshi, M. Jindal, L. Chouhan, and S. Jain, "Making drug supply chain secure traceable and efficient: a blockchain and smart contract based implementation," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 23541–23568, 2023. <https://doi.org/10.1007/s11042-022-14238-4>.
- [8] C. Wang, M. Wang, X. Wang, et al., "Multi-relational graph representation learning for financial statement fraud detection," *Big Data Mining and Analytics*, vol. 7, no. 3, pp. 920–941, 2024. <https://doi.org/10.26599/BDMA.2024.9020013>.
- [9] C. M. Naga Sudha and J. V. Nayahi, "TrackChain: Hyperledger based pharmaceutical supply chain — resource utilization perspective," *Heliyon*, vol. 10, no. 1, p. e23250, 2024. <https://doi.org/10.1016/j.heliyon.2023.e23250>.
- [10] A. Padma and M. Ramaiah, "Blockchain based solution for secure information sharing in pharma supply chain management," *Heliyon*, vol. 10, no. 22, p. e40273, 2024. <https://doi.org/10.1016/j.heliyon.2024.e40273>.

Biographies



Shamali A. Gupte is a student in the Department of Computer Engineering at St. Francis Institute of Technology (SFIT), Mumbai.



Rajkumar Shende is a faculty member in the Department of Computer Engineering at St. Francis Institute of Technology (SFIT), Mumbai.