BIOBIT: ML SECURED SUPPLY CHAIN MANAGEMENT AND DRUG AUTHENTICATION THROUGH BLOCKCHAIN

Vaani Bansal, R Navaneeth Krishnan, Punith Anand, Aditya Kumar Sinha, and Sheela Devi

Department of Computer Science Engineering, PES University, Bangalore, India

ABSTRACT

Counterfeit medicines absolutely show a high threat to public health and non-functional areas in the pharmaceutical industry that do not have proper regulatory mechanisms in place. Such counterfeit drugs might contain the wrong doses or even some hazardous materials. Hence, they break the trust formed between the healthcare system and patients and expose patients to severe health risks. This project presents a complete solution integrated with blockchain technology and machine learning features to ensure drug authenticity and to protect the pharmaceutical supply chain.

Blockchain module built on Hyperledger Fabric gives the tamper-proof, decentralized ledger for medicine logistics tracking. Each medicine has a unique QR code that links together with its whole manufacturing and regulatory information. This provides the scope for customers and employees to check medicines authenticity at the same time just by scanning the code. In other words, this encourages transparency and makes traceability, thus preventing counterfeit drugs entering the supply chain.

The protection of the blockchain infrastructure is ensured by employing an anomaly detection model using XGBoost-based machine learning. Trained on the NSL-KDD dataset, the model is capable of identifying and nullifying network malicious activities such as unauthorized access attempt, thereby ensuring reliability and security of the system.

By combining these technologies, an all-in-one, scalable solution for minimizing counterfeiting medicines is available. The data within the framework can be kept by blockchain integrity and accessibility while providing machine learning security and thus forming a complete counterfeiting regime. The system not only protects public health but also improves the culture of trust and transparency in the pharmaceutical supply chain, making it a feasible approach for large-scale implementation in the industry.

KEYWORDS

Blockchain, Machine Learning, Pharmaceutical Supply Chain, Counterfeit Drugs, Hyperledger

1. INTRODUCTION

Counterfeit drugs pose a serious threat to public health and the pharmaceutical industry, often containing incorrect dosages, harmful substances, or completely ineffective ingredients. According to the World Health Organization, one in ten medicines in underdeveloped countries is

David C. Wyld et al. (Eds): NLCAI, AIFU, CCSEA, BIoT, SEA, SIPRO, BDML, CLOUD – 2025
pp. 153-166, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151012

either counterfeit or of poor quality, leading to severe health risks, prolonged illnesses, and increased mortality rates. The economic impact is staggering, with pharmaceutical companies losing over 200 billion dollars annually due to counterfeit products eroding consumer trust and damaging brand credibility.

Advancements in technology have made it easier for counterfeiters to produce convincing fake drugs that evade detection. The global nature of pharmaceutical supply chains complicates the issue, as counterfeit medicines often cross multiple jurisdictions before reaching consumers. While developed countries invest heavily in securing their supply chains—such as the U.S., which spends around 800 billion dollars annually—traditional methods remain insufficient. Experts advocate for stricter regulations, better surveillance, and the adoption of advanced tracking technologies like blockchain to enhance transparency and security. Blockchain, a decentralized and tamper-proof ledger, can provide real-time tracking of medicines from production to distribution. Hyperledger Fabric, a permissioned blockchain, offers controlled access to ensure both security and accountability.

Additionally, integrating machine learning, such as an XGBoost-based anomaly detection model, can further enhance fraud detection. By combining these technologies, the pharmaceutical industry can take a significant step toward eliminating counterfeit drugs, protecting public health, and restoring consumer confidence.

2. RELATED WORK

Blockchain is a rapidly expanding domain centered around distributed ledger technology, enhancing integrity and transparency. It has the potential to make organizations secure, efficient, and decentralized.

2.1. Papers and Related Literature

[1] This paper discusses the use of Hyperledger Fabric for a decentralized supply chain management system. It ensures secure and transparent transactions while utilizing smart contracts to enable safe agreements without intermediaries.

[12] This paper proposes an anomaly detection method for blockchain networks, focusing on Bitcoin. It employs Auto Encoder (AE) models to detect issues in blockchain traffic in real-time. The approach enhances security by profiling typical behavior, identifying key characteristics, and optimizing detection performance with minimal resource usage.

[13] This paper presents a system using a portable digital microscope to capture QR code details, a cloud-based authenticity checker, and a fine-tuned CNN for distinguishing printed and copied QR codes. It also includes scripts for modifying QR codes, querying a registry, and embedding covert messages without altering their visible appearance.

[14] This paper integrates machine learning (XGBoost, Random Forest) with blockchain for fraud detection. The system preprocesses data, trains models to classify transactions, and embeds them in a blockchain-based smart contract, ensuring real-time classification and enhanced security through decentralization.

3. Proposed Methodology for Blockchain-Based Drug Supply Chain Management

3.1. Supply Chain Transparency and Drug Authentication Framework

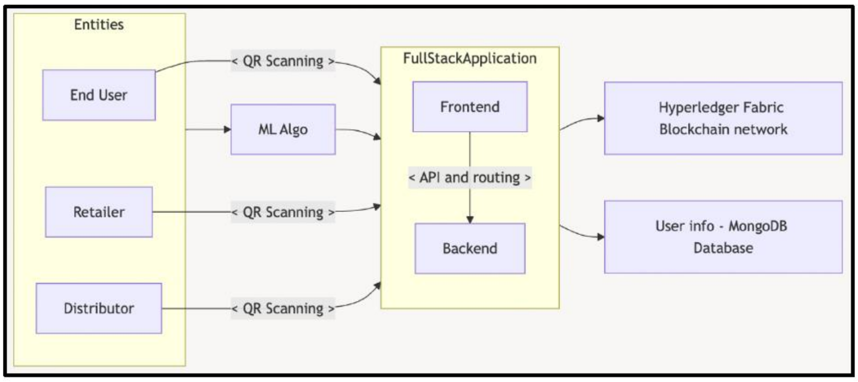


Figure 1. Flow chart of methodology

Our proposed methodology addresses the critical challenges of supply chain transparency and drug authentication using a Hyperledger Fabric Blockchain network. This permissioned blockchain ensures secure and immutable recording of transactions throughout the supply chain, while also enabling real-time traceability. The system integrates blockchain with machine learning and full-stack web development technologies to enhance usability and robustness.

3.2. Full-Stack Architecture

The application architecture is designed to deliver a seamless user experience and efficient backend operations.

1.Frontend: The user interface is developed using React to provide a sleek and intuitive experience. Key features include login authentication, drug QR code scanning, and access to drug details, enabling users to verify the legitimacy of a drug.

2.Backend: The backend is built using Express and Node.js, ensuring responsiveness and API-friendly architecture. It acts as the intermediary between the frontend, blockchain network, and database, managing API routing and data processing efficiently.

3.Blockchain Integration: Hyperledger Fabric is utilized as the blockchain framework, providing a permissioned environment that guarantees data immutability and secure traceability. Only authorized entities, such as regulatory authorities, are part of the network, ensuring compliance and integrity. Users access data such as product and drug details through APIs, without directly interacting with the blockchain.

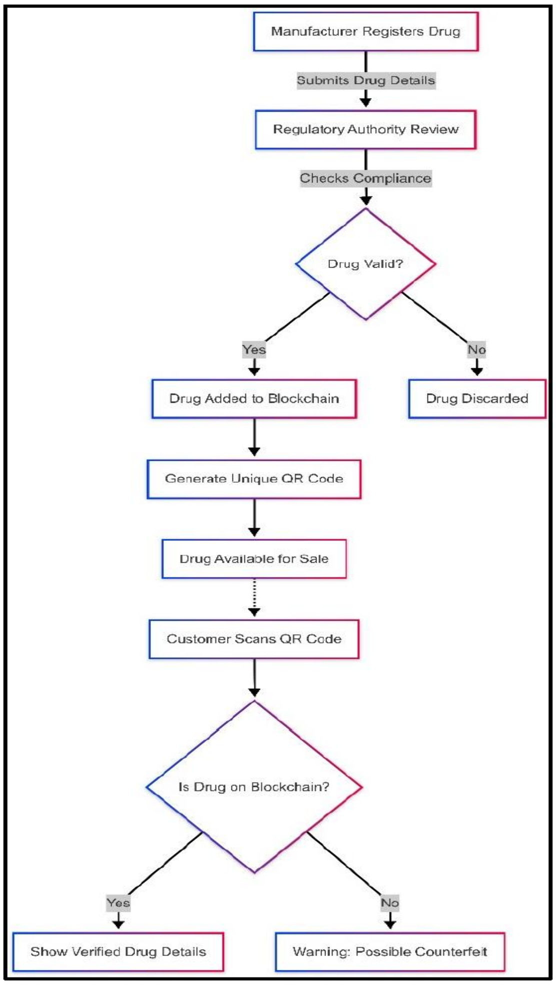


Figure 2. State Diagram of Data Sources and Interactions in Blockchain

4.Database: MongoDB is employed to store user details and QR code metadata. Its document-oriented data model is optimal for handling the unstructured and hierarchical data generated in the application, offering flexibility and scalability.

4. INTRUSION DETECTION ARCHITECTURE

The machine learning component of the capstone project involves protecting the full-stack application through an anomaly detection mechanism implemented using the XGBoost algorithm. The model is trained on the NSL-KDD dataset, which is labeled network traffic data with attributes such as protocol type, duration, source/destination IP, service type, flag status, and other packet statistics. The main objective is to identify incoming packets as normal or anomalous in real time. The data is preprocessed during training to balance class distribution, normalize numeric features, and encode categorical features for stable model performance.

The trained XGBoost model is implemented at the application gateway to screen all incoming requests prior to their interaction with the system. Password-sanitized requests alone from the full-stack application are permitted to access the blockchain, while suspicious packets potentially indicative of attacks like DoS attacks, probing, or unauthorized access are flagged and terminated. In the event of an unauthorized access attempt, the system notifies the requisite SDK services to respond to security protocols and adjust corresponding resources accordingly. This proactive monitoring improves application security by inhibiting unauthorized access and guarding confidential data. Model performance is intermittently evaluated on precision, recall, and F1 score measurements, and the model is retaught using new data to evolve with developing threats.

Dataset:

The NSL-KDD dataset, which is a filtered version of the KDD Cup 1999 dataset, is utilized in this project. The dataset includes labeled network traffic data comprising 41 attributes, including both continuous attributes (e.g., connection time, failed logins) and categorical attributes (e.g., protocol, service type). The traffic is categorized into five types based on the dataset: DoS, R2L, U2R, Probe, and normal traffic. The dataset is divided into train and test sets, with removal of duplicate records for more authentic analysis.

Data Preprocessing:

Network traffic data is collected using TShark in real time. Data is then cleaned and filtered to remove packet information not relevant to network analysis and noise. Feature extraction isolates key characteristics such as packet timing and flow rates to ensure effective anomaly detection. Missing data is treated via imputation or exclusion, and features are normalized or scaled to produce well-balanced model performance. Preprocessed data is then divided into training and test sets for model testing.

XGBoost:

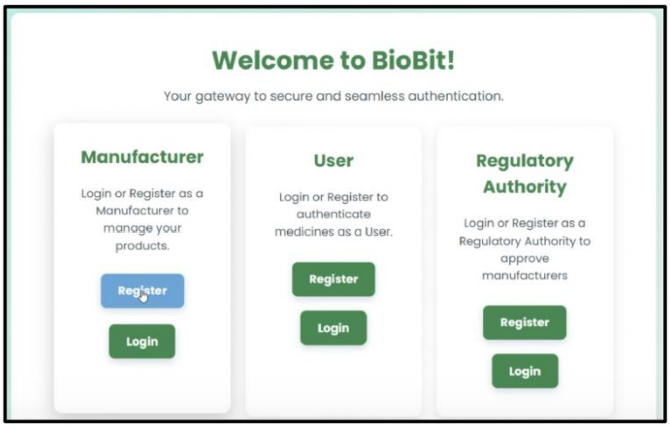
XGBoost is utilized for classifying network traffic and anomaly detection. It is trained on the NSL-KDD dataset to determine malicious patterns like DDoS attacks or illegal access attempts. The model is based on a gradient boosting paradigm to blend weak models and construct a powerful, efficient system for real-time detection of threats.

TShark:

TShark constantly monitors network traffic and marks suspicious patterns. Upon detecting anomalies, administrators are notified for immediate examination, and the system calls SDK services to manage security responses in real-time. Proactive monitoring secures the entire-stack application and guarantees that only authenticated requests communicate with the blockchain. By blocking unauthorized access, DDoS attacks, and other malicious attempts before they even hit Hyperledger Fabric, the system improves overall trust and security.

5. Implementation of AI Secured Supply Chain Management and Drug Authentication through Blockchain

This is a blockchain-and-machine-learning integrated system that strengthens a full-stack application by secure and intact methods, ensuring privacy in data used in the supply chain pharmaceuticals’ systems. Hyperledger Fabric’s decentralized immutable nature integrates



Welcome to BioBit!

Your gateway to secure and seamless authentication.

Manufacturer

Login or Register as a Manufacturer to manage your products.

User

Login or Register to authenticate medicines as a User.

Regulatory Authority

Login or Register as a Regulatory Authority to approve manufacturers

Figure 3. Role-based interfaces on landing page

anomaly detection, involving machine learning, which particularly uses XGBoost algorithms, against cyber threats in the pharmaceutical supply chain systems.

The blockchain component of the system applies Hyperledger Fabric to create a transparent and secure supply chain network. This blockchain network will involve stakeholders such as raw material suppliers, manufacturers, distributors, pharmacies, and hospitals, where transactions related to drug production and distribution can be made tamper-proof and easily auditable. Hyperledger Fabric enforces and ensures rules and regulations across this network. This means ensuring that all participants in the value chain are compliant with regulations, standards, and control measures regarding drug verification or origin and regulatory compliance, among others.

In line with blockchain, the system employed machine learning to monitor this network traffic for potential threats. TShark, an analyzer of network protocol, collects real-time packet data from the network through preprocessing and feeds it into an XGBoost model. The model is trained on normal and anomalous patterns of traffic so that it will identify possible security threats where the integrity of the data stored in the blockchain may get compromised. When the system detects anyabnormal activity, it sends alerts to the administrators to take proactive security measures.This will ensure the application is protected from vulnerabilities and hazardous activities.

A safe, transparent, and reliable pharmaceutical supply chain system comes with the integration of blockchain with machine learning. The network ensures data integrity and traceability while the model scans the networks for vulnerabilities in advance, correcting any problem found. Such a multilevel security mechanism enhances overall system trustworthiness and strengthens it against cyber threats. Following are the key components in the Hyperledger Fabric network and their interactions:

Components & Interactions:

- Peer Nodes: Validate and commit transactions.
- Orderer Nodes: Ensure consensus and create blocks.
- Certificate Authority (CA): Issues digital certificates for identity management.
- Smart Contracts (Chaincode): Executes business logic.
- CouchDB: Stores the latest state of the blockchain.

- External Applications (APIs, Frontend Clients): Query blockchain data.
- Participants: Manufacturers, Distributors, Retailers, Regulators, and Consumers.

Interaction Flow:

- Manufacturer submits drug details via API.
- Peer nodes validate and endorse the transaction.
- Orderer nodes package validated transactions into blocks.
- Blocks are added to the blockchain, updating CouchDB.
- Consumers verify drugs by scanning QR codes, querying the blockchain

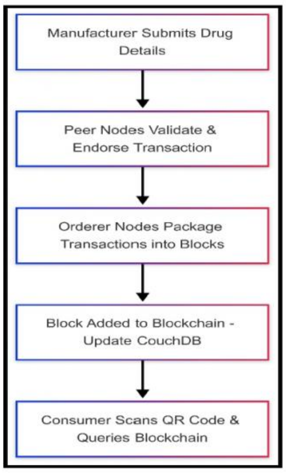
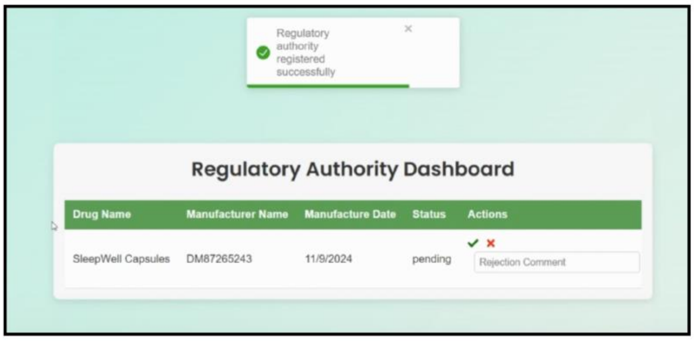

Manufacturer Submits Drug Details
Peer Nodes Validate & Endorse Transaction
Orderer Nodes Package Transactions into Blocks
Block Added to Blockchain - Update CouchDB
Consumer Scans QR Code & Queries Blockchain

Figure 4. Logical Interaction Diagram

5.1. User Registration and Login

1. Registration: Manufacturers and regulatory authorities (RA) register through their respective portals. Upon successful registration, RA users are automatically redirected to their dashboard, eliminating the need for an initial login.

2. Database Updates: The details of registered users are stored in the MongoDB database, reflecting real-time updates.



Regulatory authority registered successfully

Regulatory Authority Dashboard

Drug Name	Manufacturer Name	Manufacture Date	Status	Actions
SleepWell Capsules	DM87265243	11/9/2024	pending	✓ ✗ Rejection Comment

Figure 5. RA Dashboard after successful login

3. Login: Registered manufacturers log into their accounts and access the dashboard.
4. End user login/ Sign up: The end user can login to verify the authenticity of their drug, scan or upload a QR code and receive validation on the same.

5.2. Drug Addition and Approval Process

1.Drug Registration by Manufacturer: Manufacturers use their dashboard to add new drugs by scanning a QR code. They input details such as drug name, manufacturing date, and other relevant information. The details are then submitted to the RA for approval.

2.RA Approval Process: The drugs submitted are displayed on the RA's dashboard, where they can approve or reject the drugs. Upon approval, the drug information is added to the blockchain, ensuring immutability and traceability.

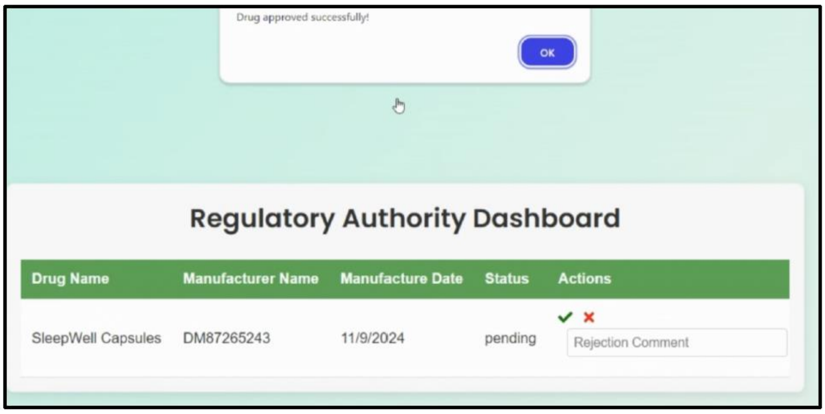
5.3. Drug Details Addition into the Blockchain

Inclusion of drug details, with the QR provided by the manufacturer is only done after the authority has checked and the peer node validation in the hyperledger. Hyperledger fabric runs a Byzantine fault tolerance system innately, making it a fault tolerant system.

The details provided by the manufacturer are stored on a MongoDB document, in order to populate the details in the regulatory authority dashboard, on approval which is then added into the fabric, in the form of key value pairs.

The QR provided by the manufacturer/ distributor is then hashed and stored for easy comparison in real time. When the end user queries the fabric, the QR provided by the end user is hashed and compared with the hashed QRs present in the fabric, if there is a match, details with regard to the respective drug is displayed, else an error message/ warning is specified to alert the user/ customer of the possible harmful effects.
This workflow demonstrates seamless collaboration between manufacturers and regulatory authorities, ensuring that only approved and authenticated drugs are added to the blockchain.

Hyperledger Addition Process: Approved drugs are added into the Hyperledger. The system successfully integrates Hyperledger Fabric to store approved drugs securely. Upon approval, the


Drug approved successfully!

Regulatory Authority Dashboard

Drug Name	Manufacturer Name	Manufacture Date	Status	Actions
SleepWell Capsules	DM87265243	11/9/2024	pending	✓ ✗ Rejection Comment

Figure 6. RA Approval and Triggering addition to HyperLedger Fabric

drug's details, including the QR code, are added to the blockchain. This ensures an immutable record of each drug entry, enhancing traceability and authenticity. The process flow from MongoDB to Hyperledger was validated to operate seamlessly without data discrepancies.

a) *./network.sh up createChannel -c mychannel -ca* : This command starts the Hyperledger Fabric network, creates a channel called *mychannel*, and sets up Certificate Authorities (CA) for the network. The *-ca* flag ensures that Fabric's Certificate Authorities are also initialized.

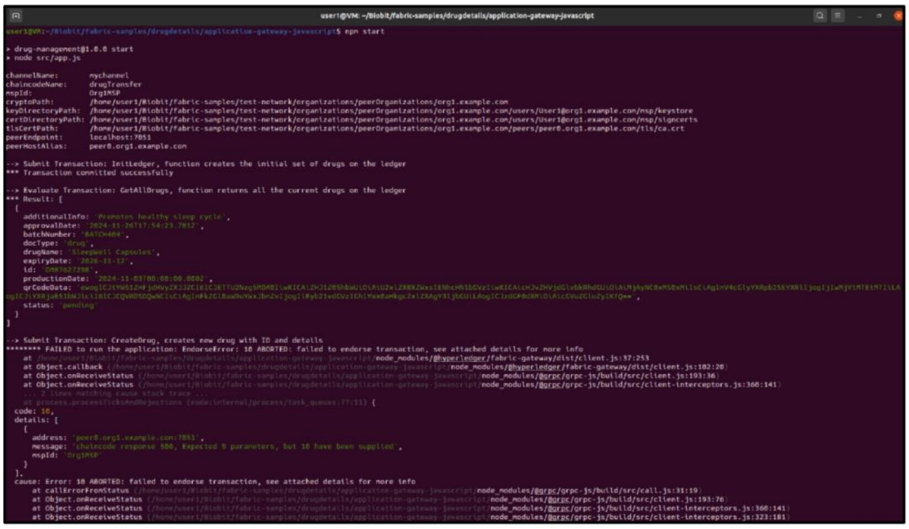
b) *./network.sh deployCC -ccn drugTransfer -ccp ../drugdetails/chaincode-javascript/ -ccl javascript* : This command deploys the *drugTransfer* chaincode on the Fabric network.

- *-ccn drugTransfer*: Specifies the chaincode name as *drugTransfer*.
- *-ccp ../drugdetails/chaincode-javascript/*: Specifies the path to the chaincode, in this case, written in JavaScript.
- *-ccl javascript*: Defines the chaincode language as JavaScript.

c) *npm start* (in the *application-gateway-javascript* folder) : This command starts the Node.js application, typically used for interacting with the Fabric network or front-end operations in your gateway. It initializes the gateway's services and API calls to the Fabric network.

d) *peer chaincode invoke ...* : This command invokes a function (in this case, *CreateDrug*) on the deployed chaincode (d*rugTransfer*) on the Hyperledger Fabric network.
The invocation specifies:

- *-o localhost:7050*: The orderer address (Fabric's ordering service node).
- *--tls:* Enabling TLS for secure communication.
- *-C mychannel*: Specifies the channel to invoke the chaincode on (*mychannel*).
- *-n drugTransfer*: Specifies the chaincode name (*drugTransfer*).
- *-c '{"function":"CreateDrug","Args":[...]}'*: Specifies the chaincode function and the arguments (e.g., drug details) to pass to the function.



user1@VM: ~/Biobit/fabric-samples/drugdetails/application-gateway-javascript

```
user1@VM:~/Biobit/fabric-samples/drugdetails/application-gateway-javascript$ npm start

> drug-management@1.0.0 start
> node src/app.js

channelName:       mychannel
chaincodeName:     drugTransfer
mspId:             Org1MSP
cryptoPath:        /home/user1/Biobit/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com
keyDirectoryPath:  /home/user1/Biobit/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/keystore
certDirectoryPath: /home/user1/Biobit/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/signcerts
tlsCertPath:       /home/user1/Biobit/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt
peerEndpoint:      localhost:7051
peerHostAlias:     peer0.org1.example.com

--> Submit Transaction: InitLedger, function creates the initial set of drugs on the ledger
*** Transaction committed successfully

--> Evaluate Transaction: GetAllDrugs, function returns all the current drugs on the ledger
*** Result: [
  {
    additionalInfo: 'Promotes healthy sleep cycle',
    approvalDate: '2024-11-26T17:54:23.781Z',
    batchNumber: 'BATCH404',
    docType: 'drug',
    drugName: 'SleepWell Capsules',
    expiryDate: '2026-11-12',
    id: 'DM87627290',
    productionDate: '2024-11-03T00:00:00.000Z',
    qrCodeData: '[illegible]',
    status: 'pending'
  }
]

--> Submit Transaction: CreateDrug, creates new drug with ID and details
******** FAILED to run the application: EndorseError: 10 ABORTED: failed to endorse transaction, see attached details for more info
    at /home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@hyperledger/fabric-gateway/dist/client.js:37:253
    at Object.callback (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@hyperledger/fabric-gateway/dist/client.js:102:20)
    at Object.onReceiveStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/client.js:193:36)
    at Object.onReceiveStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/client-interceptors.js:360:141)
    ... 2 lines matching cause stack trace ...
    at process.processTicksAndRejections (node:internal/process/task_queues:77:11) {
  code: 10,
  details: [
    {
      address: 'peer0.org1.example.com:7051',
      message: 'chaincode response 500, Expected 9 parameters, but 10 have been supplied',
      mspId: 'Org1MSP'
    }
  ],
  cause: Error: 10 ABORTED: failed to endorse transaction, see attached details for more info
      at callErrorFromStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/call.js:31:19)
      at Object.onReceiveStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/client.js:193:76)
      at Object.onReceiveStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/client-interceptors.js:360:141)
      at Object.onReceiveStatus (/home/user1/Biobit/fabric-samples/drugdetails/application-gateway-javascript/node_modules/@grpc/grpc-js/build/src/client-interceptors.js:323:181)
```

Figure 7. Adding drug details into the Hyperledger

On successful addition of an approved drug into the Hyperledger, the end user can scan the QR, either through a manual camera scan or upload, and if there is a match in the QR code data, in the scanned image and drug details in the Hyperledger, it displays the drug details accordingly.

5.4. Counterfeit Drug Detection

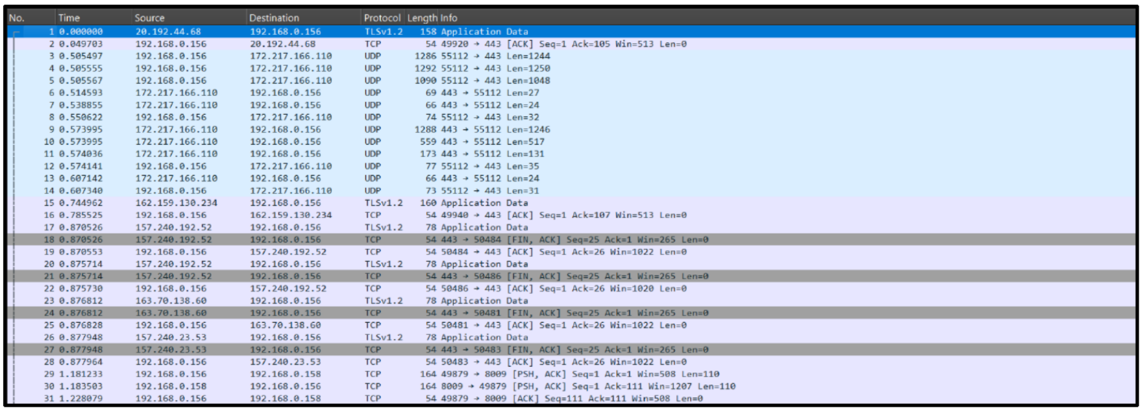
Drug Transparency: Drugs that fail regulatory approval or are not added to the blockchain are flagged as potential counterfeits. This helps streamline the identification process and provides actionable insights to prevent the circulation of unverified drugs in the supply chain.

Table 1. Data Flow & Dependency Table for Tamper-Proof Decentralized Register

Parameter	**Source**	**Usage**
Identity Role	Certificate Authority (CA)	Assigns access control (Manufacturer, Regulator, etc.)
Transaction Timestamp	Blockchain Ledger	Ensures transaction immutability
Drug ID	Manufacturer Entry	Unique identifier for the product
Batch Number	Manufacturer Entry	Tracks product batches
Regulatory Status	Regulator Input	Compliance check status
Hash of Previous Transactions	Blockchain Ledger	Ensures tamper-proof integrity
Digital Signature	Smart Contract	Provides transaction authentication
ML-Based Intrusion Detection Score	Machine Learning Module	Flags potential fraud

5.5. Intrusion Detection System

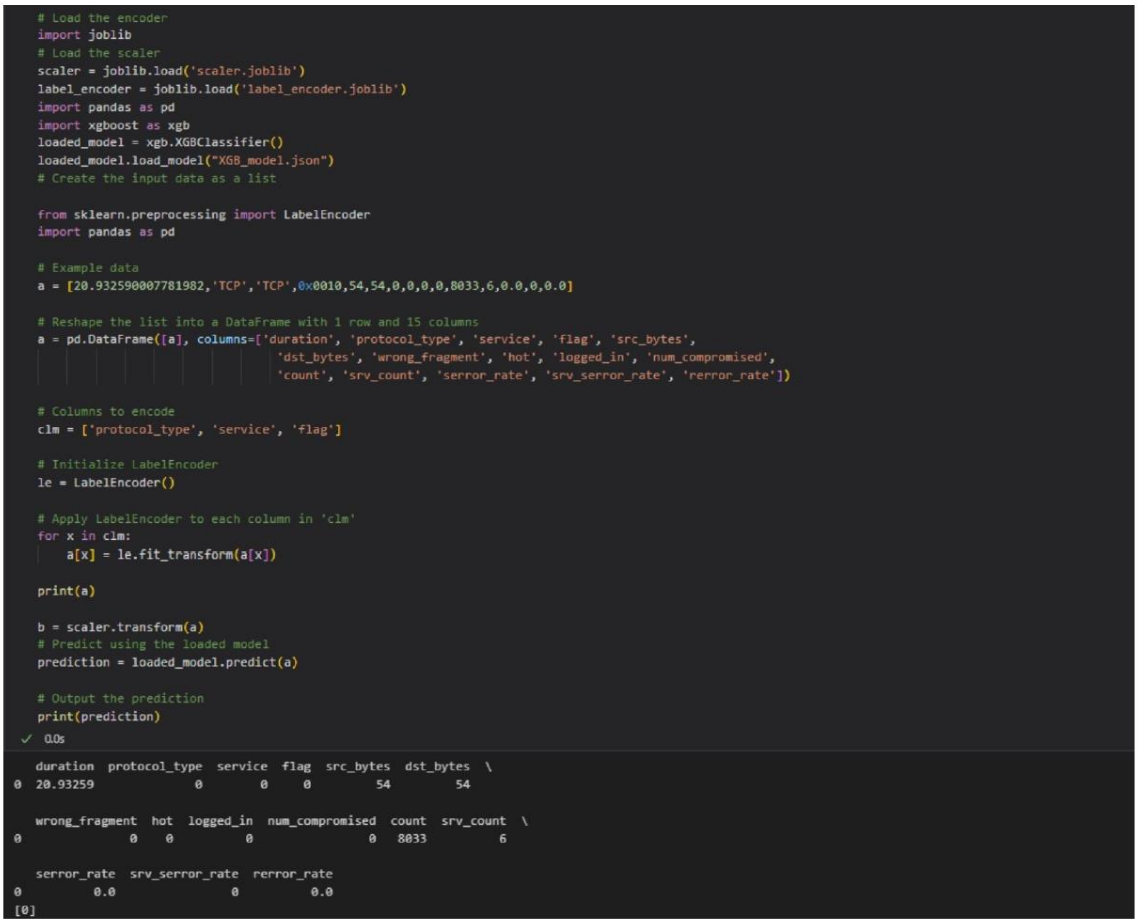
The system employs a machine learning (ML) model to continuously monitor network traffic and detect anomalies in real time. When an anomalous packet is identified, the system generates detailed log files that document the nature of the anomaly, affected network parameters, and potential security risks. These logs are made available for network administrators to analyze,



```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   20.192.44.68     192.168.0.156    TLSv1.2   158 Application Data
   2 0.049703   192.168.0.156    20.192.44.68     TCP        54 49920 → 443 [ACK] Seq=1 Ack=105 Win=513 Len=0
   3 0.505497   192.168.0.156    172.217.166.110  UDP      1286 55112 → 443 Len=1244
   4 0.505555   192.168.0.156    172.217.166.110  UDP      1292 55112 → 443 Len=1250
   5 0.505567   192.168.0.156    172.217.166.110  UDP      1090 55112 → 443 Len=1048
   6 0.514593   172.217.166.110  192.168.0.156    UDP        69 443 → 55112 Len=27
   7 0.538855   172.217.166.110  192.168.0.156    UDP        66 443 → 55112 Len=24
   8 0.550622   192.168.0.156    172.217.166.110  UDP        74 55112 → 443 Len=32
   9 0.573995   172.217.166.110  192.168.0.156    UDP      1288 443 → 55112 Len=1246
  10 0.573995   172.217.166.110  192.168.0.156    UDP       559 443 → 55112 Len=517
  11 0.574036   172.217.166.110  192.168.0.156    UDP       173 443 → 55112 Len=131
  12 0.574141   192.168.0.156    172.217.166.110  UDP        77 55112 → 443 Len=35
  13 0.607142   172.217.166.110  192.168.0.156    UDP        66 443 → 55112 Len=24
  14 0.607340   192.168.0.156    172.217.166.110  UDP        73 55112 → 443 Len=31
  15 0.744962   162.159.130.234  192.168.0.156    TLSv1.2   160 Application Data
  16 0.785525   192.168.0.156    162.159.130.234  TCP        54 49940 → 443 [ACK] Seq=1 Ack=107 Win=513 Len=0
  17 0.870526   157.240.192.52   192.168.0.156    TLSv1.2    78 Application Data
  18 0.870526   157.240.192.52   192.168.0.156    TCP        54 443 → 50484 [FIN, ACK] Seq=25 Ack=1 Win=265 Len=0
  19 0.870553   192.168.0.156    157.240.192.52   TCP        54 50484 → 443 [ACK] Seq=1 Ack=26 Win=1022 Len=0
  20 0.875714   157.240.192.52   192.168.0.156    TLSv1.2    78 Application Data
  21 0.875714   157.240.192.52   192.168.0.156    TCP        54 443 → 50486 [FIN, ACK] Seq=25 Ack=1 Win=265 Len=0
  22 0.875730   192.168.0.156    157.240.192.52   TCP        54 50486 → 443 [ACK] Seq=1 Ack=26 Win=1020 Len=0
  23 0.876812   163.70.138.60    192.168.0.156    TLSv1.2    78 Application Data
  24 0.876812   163.70.138.60    192.168.0.156    TCP        54 443 → 50481 [FIN, ACK] Seq=25 Ack=1 Win=265 Len=0
  25 0.876828   192.168.0.156    163.70.138.60    TCP        54 50481 → 443 [ACK] Seq=1 Ack=26 Win=1022 Len=0
  26 0.877948   157.240.23.53    192.168.0.156    TLSv1.2    78 Application Data
  27 0.877948   157.240.23.53    192.168.0.156    TCP        54 443 → 50483 [FIN, ACK] Seq=25 Ack=1 Win=265 Len=0
  28 0.877964   192.168.0.156    157.240.23.53    TCP        54 50483 → 443 [ACK] Seq=1 Ack=26 Win=1022 Len=0
  29 1.181233   192.168.0.156    192.168.0.158    TCP       164 49879 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=508 Len=110
  30 1.183503   192.168.0.158    192.168.0.156    TCP       164 8009 → 49879 [PSH, ACK] Seq=1 Ack=111 Win=1207 Len=110
  31 1.228079   192.168.0.156    192.168.0.158    TCP        54 49879 → 8009 [ACK] Seq=111 Ack=111 Win=508 Len=0
```

Figure 8. Captured Network Traffic

review, and take appropriate countermeasures. Additionally, if an anomaly suggests a potential security breach, the system contacts SDK services to trigger adaptive security responses.



```
# Load the encoder
import joblib
# Load the scaler
scaler = joblib.load('scaler.joblib')
label_encoder = joblib.load('label_encoder.joblib')
import pandas as pd
import xgboost as xgb
loaded_model = xgb.XGBClassifier()
loaded_model.load_model("XGB_model.json")
# Create the input data as a list

from sklearn.preprocessing import LabelEncoder
import pandas as pd

# Example data
a = [20.932590007781982,'TCP','TCP',0x0010,54,54,0,0,0,0,8033,6,0.0,0,0.0]

# Reshape the list into a DataFrame with 1 row and 15 columns
a = pd.DataFrame([a], columns=['duration', 'protocol_type', 'service', 'flag', 'src_bytes',
                                'dst_bytes', 'wrong_fragment', 'hot', 'logged_in', 'num_compromised',
                                'count', 'srv_count', 'serror_rate', 'srv_serror_rate', 'rerror_rate'])

# Columns to encode
clm = ['protocol_type', 'service', 'flag']

# Initialize LabelEncoder
le = LabelEncoder()

# Apply LabelEncoder to each column in 'clm'
for x in clm:
    a[x] = le.fit_transform(a[x])

print(a)

b = scaler.transform(a)
# Predict using the loaded model
prediction = loaded_model.predict(a)

# Output the prediction
print(prediction)
```

```
   duration  protocol_type  service  flag  src_bytes  dst_bytes  \
0  20.93259              0        0     0         54         54

   wrong_fragment  hot  logged_in  num_compromised  count  srv_count  \
0               0    0          0                0   8033          6

   serror_rate  srv_serror_rate  rerror_rate
0          0.0                0          0.0
[0]
```

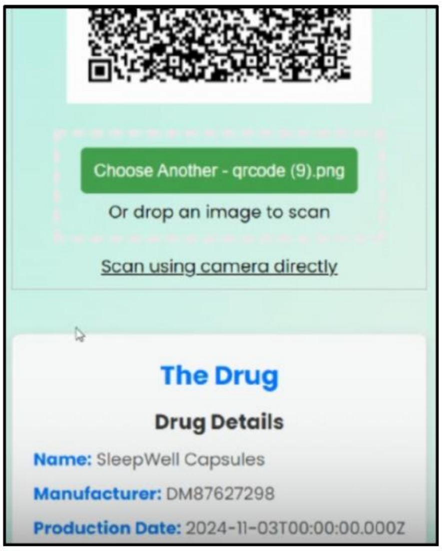
Figure 9. Working of ML Model

By proactively detecting and logging suspicious activity, the system ensures uninterrupted operation even during low-level network attacks, effectively mitigating potential threats and fortifying the full-stack application against unauthorized access.

.

6. RESULTS AND DISCUSSION

This implementation of an anti-counterfeiting system was proven to be a system with superior integrity and improved transparency in the supply chain management process. Using TShark,



The Drug

Drug Details

Name: SleepWell Capsules

Manufacturer: DM87627298

Production Date: 2024-11-03T00:00:00.000Z

Figure 10. User Scanning with Drug details

which is the terminal-based network protocol analyzer, captures and analyzes the network traffic.

This utility tool extracts the features or particular attributes from packet data to feed them into the process of anomaly detection. These preprocessed attributes are fed into an XGBoost-based machine learning model that is trained with the NSL-KDD dataset for normal or anomalous classification of packets. TShark's efficiency with real-time packet analysis makes it an integrated part of your threat detection pipeline, ensuring comprehensive data for accurate model predictions.

This enables a backend API to trigger the Fabric SDK and add drug details into the Hyperledger.

6.1. QR Code-Based Drug Verification

1. End User QR Scanning: Users can scan the QR code associated with a drug to retrieve its details from the blockchain. The system performs efficient lookup using base64-encoded QR code data. Tests confirmed that drug verification is accurate and response times are within acceptable limits, ensuring reliability during end-user interactions.

2. TShark captures live network traffic and extracts important features, such as protocol types, IPs, and ports. Data from the output of TShark is then cleaned, normalized, and encoded to suit the needs of the XGBoost model for analysis. After the pre-processing stage, the data is analyzed by the model to determine whether a packet is anomalous or normal. All logged anomalies trigger an alert; TShark, therefore, becomes a crucial element that translates raw traffic into meaningful, actionable threat intelligence. This data is then sent to the ML model to make predictions.

The implementation of a QR-based Hyperledger-powered supply chain management system is a novel approach to providing a transparent and immutable solution against counterfeiting and improving the tracking process.

7. CONCLUSION AND FUTURE SCOPE

Our blockchain-based drug supply chain management system, augmented with AI-driven anomaly detection which functions as an intrusion detection system, notifies the network admin in the case of any network intrusion. It provides a secure and efficient solution to counteract counterfeit drugs, enhance regulatory compliance, and ensure transparency across the pharmaceutical supply chain. By leveraging blockchain's immutability and AI's analytical capabilities, the system enables real-time drug authentication and proactive threat detection, empowering stakeholders to make informed decisions and safeguard pharmaceutical integrity.

The future scope of this project is wide-ranging and holds promising potential for advancements in the field of blockchain and ML for supply chain management. Some key areas for future development and research include:

1. Scalability Enhancements: Optimize system performance using techniques like sharding, load balancing, and advanced querying to handle higher volumes of data and users.

2. Integration with Other Blockchain Platforms: Enable interoperability with platforms like Ethereum or Corda and support cross-chain data exchange for improved verification.

3. Advanced Machine Learning Models: Incorporate hybrid or transformer-based models to enhance anomaly detection and adapt to evolving cyber threats.

4. Mobile Application: Develop a user-friendly mobile app for offline QR code scanning and drug authenticity verification.

REFERENCES

[1] Abbas, K.; Afaq, M.; Ahmed Khan, T.; Song, W.C. A Blockchain and Machine Learning Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry. Electronics 2020, 9, 852. https://doi.org/10.3390/electronics9050852

[2] Alari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catal˜ao, J.P. A review of smart cities based on the internet of things concept. Energies 2017, 10, 421. [Google Scholar] [CrossRef] [Green Version]

[3] Khan, P.W.; Byun, Y.; Namje, P. A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. Electronics 2020, 9, 484

[4] Liu, X.; Wang, W.; Guo, H.; Barenji, A.V.; Li, Z.; Huang, G.Q. Industrial blockchain based

[5] framework for product lifecycle management in industry 4.0. Robot. Comput. Integr. Manuf. 2020, 63, 101897 Ke, G.; Meng, Q.; Finley, T.; Wang, T.; Chen, W.; Ma, W.; Ye, Q.;

[6] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[9] Liu, T.Y. Lightgbm: A highly efficient gradient boosting decision tree. In Advances in Neural Information Processing Systems 30; Curran Associates, Inc.: Dutchess County, NY, USA, 2017; pp. 3146-3154

[10] Wu, T.Y.; Fan, X.; Wang, K.H.; Lal, C.F.; Xiong, N.; Wu, J.M.T. A DNA Computation-Based Image Encryption Scheme for Cloud CCTV Systems. IEEE Access 2019, 7, 181434-181443. [Google Scholar]

[11] Wu, X.; Lin, Y. Blockchain recall management in pharmaceutical industry.Procedia CIRP 2019, 83, 590-595 Rabah, K. Challenges & opportunities for blockchain powered healthcare systems: A review. Mara Res. J. Med. Health Sci. 2017, 1, 45-52.

[12] Williams, L.; McKnight, E. The real impact of counterfeit medications. US Pharm. 2014, 39, 44-46.

[13] J. Kim et al., "A Machine Learning Approach to Anomaly Detection Based on Traffic Monitoring for Secure Blockchain Networking"

[14] An Innovative Method for Securing QR Codes against Counterfeits in Supply Chain Management Richard Wu. Nicole Liu.Grace Peng.Adarsha Bhattarai,Dongming Peng

[15] A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism Tehrcem Ashfaq 1, Rabyta Khalid 1, Adamu Sani Yahaya 1,2, Sheraz Aslam 3,4 , Ahmad Taher Azar 4,5,6,. ,Safa Alsafari 7 and Ibrahim A. Hameed