Demo: Enabling Trustworthy Cold Chain Logistics through Blockchain and Machine Learning

Rashmi Ratnayake*, Madhusanka Liyanage†, Liam Murphy‡
*†‡School of Computer Science, University College Dublin, Ireland
Email: *rashmi.ratnayake@ucdconnect.ie, †madhusanka@ucd.ie, ‡liam.murphy@ucd.ie

***Abstract*—Internet of Things (IoT) sensors monitor temperature-sensitive goods throughout the supply chain. Nowadays, blockchain is being widely used for traceability, transparency, and immutable storage of this data. However, this approach lacks a mechanism to assess the trustworthiness of the data, and as a result, the reliability of the system is constrained by the quality of the data being added. IoT sensor data can be compromised for various reasons, including sensor malfunctions, deliberate tampering, or human error. This demonstration presents a solution that integrates machine learning techniques with blockchain to enhance data trust in cold chain logistics.**

***Index Terms*—IoT, Supply Chain, Data Trustworthiness, Blockchain, Machine Learning, Smart Contracts**

I. Introduction

The cold chain logistics industry faces a significant challenge in maintaining precise environmental conditions throughout the supply chain, especially when transporting temperature-sensitive products like vaccines and perishable food [1]. Even a brief deviation from the required temperature range can lead to product spoilage or render goods unusable, resulting in significant financial losses and posing serious health risks to the public. To mitigate these risks, Internet of Things (IoT) temperature sensors continuously monitor the storage environment of these sensitive goods, recording data in real time. While blockchain technology is increasingly employed to provide immutability and transparency of this supply chain data, ensuring data accuracy goes beyond simply enabling traceability and secure storage. It is crucial to verify that the data itself is trustworthy and reliable. In order to solve this, we suggest a solution that combines IoT temperature sensors, blockchain technology, machine learning and edge computing to guarantee the accuracy of environmental data through the supply chain.

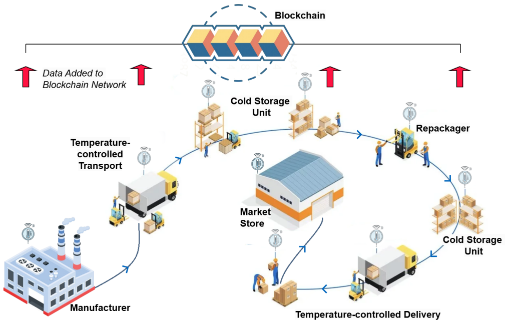

Blockchain
Data Added to Blockchain Network
Cold Storage Unit
Repackager
Temperature-controlled Transport
Market Store
Cold Storage Unit
Manufacturer
Temperature-controlled Delivery

Fig. 1: Blockchain and IoT-Enabled Cold Chain Logistics

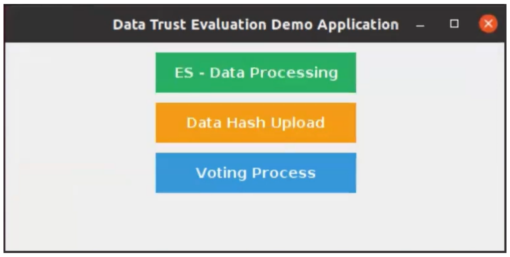


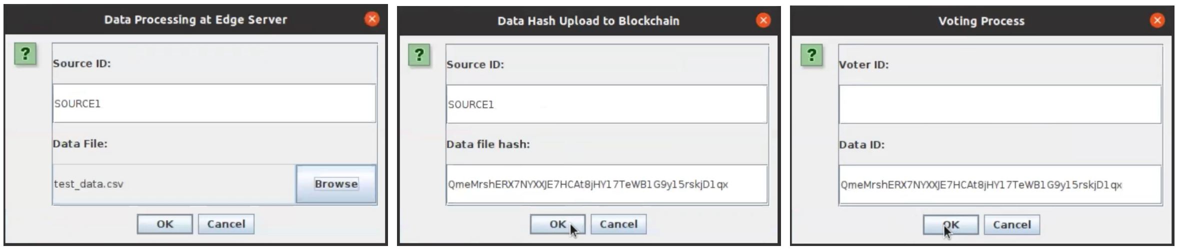
Fig. 2: Main Interface of the System Prototype

II. System Architecture

In this system, IoT temperature sensors are embedded within refrigerated trucks, storage units, and warehouses to monitor temperature conditions continuously. These sensors are deployed at various critical points along the supply chain, ensuring real-time data capture of the conditions in which goods are stored or transported. The collected data is transmitted to edge servers located at distribution centres or transportation hubs, which act as preliminary trust evaluators and blockchain nodes. The role of these edge servers is pivotal as they perform initial data checks, filter out anomalies, and assign trust labels to the incoming data. This is done using a pre-trained Support Vector Machine (SVM) model, followed by a trust score calculation employing decision scores from the SVM models and reputation scores of the data source.

Once the data has undergone this initial evaluation, it is uploaded to the InterPlanetary File System (IPFS) and the hashes are stored in a blockchain network. Blockchain validators perform a deeper level of verification on the data entries that are likely to have been misclassified during the preliminary validation. These validators use multiple machine learning models to conduct trustworthiness assessments on the data and submit their evaluations as votes. Based on a majority consensus from the validators, the final trust labels for the data entries are determined through a smart contract. If discrepancies are identified between the trust labels assigned by the edge servers and those determined by the validators, new entries with corrected labels are added to the blockchain. The detailed algorithms are introduced in [2].

This approach uses blockchain technology not only for tamper-proof data storage but also for distributed validation of data records, creating a trustworthy, transparent record of environmental conditions. By integrating IPFS for off-chain storage, the system becomes more scalable and enables the efficient distribution of large amounts of data, reducing duplication compared to traditional blockchain systems.


Data Processing at Edge Server
?
OK
Cancel
Data Hash Upload to Blockchain
?
OK
Cancel
Voting Process
?
OK
Cancel

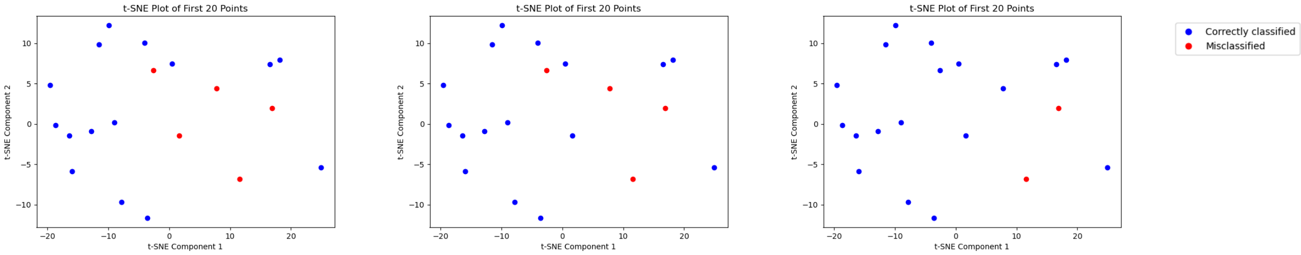
Source ID: SOURCE1
Data File: test_data.csv Browse

Source ID: SOURCE1
Data file hash: QmeMrshERX7NYXXJE7HCAt8jHY17TeWB1G9y15rskjD1qx

Voter ID:
Data ID: QmeMrshERX7NYXXJE7HCAt8jHY17TeWB1G9y15rskjD1qx

(a) Edge Server Interface (b) Data Upload Interface (c) Vote Submission Interface

Fig. 3: Prototype Interfaces



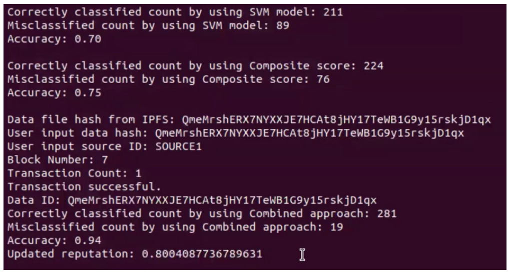
(a) Using SVM (b) Using Composite Trust Score (c) Using Combined ML Model Approach

Fig. 4: Data Evaluation Outputs

The demonstration presents a prototype developed to illustrate the proposed solution. Blockchain development was implemented in Java using Hyperledger Fabric v2.4.4, while the machine learning models were built in Python. A Java Swing application was created to provide user interfaces for the primary actions performed by the edge servers and validators, allowing interaction with the blockchain smart contract backend. Fig. 2 shows the main interface of the prototype, while the additional interfaces are presented in Fig. 3.

Temperature readings from the Intel Lab dataset [3] were used for the demonstration with faulty data generated using the Random Walk Infilling algorithm proposed in [4]. Validators on the blockchain use 3 machine learning models - K-Nearest Neighbors, Random Forest, and Multilayer Perceptron. It is assumed that these models are used in equal proportions during the validation process.

The results demonstrate a significant improvement in data classification accuracy through the use of the composite trust score and combined approaches, as shown in Fig. 4. Both these results, along with the reputation update, are displayed in the Command Line Interface (CLI) output in Fig. 5. The experiments using the combined ML model approach reveal substantial gains in accurately assessing the trustworthiness of the data. Furthermore, the end-to-end latency experiments show that the trust evaluation process can be completed in an acceptable time frame, typically within a few seconds.



```
Correctly classified count by using SVM model: 211
Misclassified count by using SVM model: 89
Accuracy: 0.70

Correctly classified count by using Composite score: 224
Misclassified count by using Composite score: 76
Accuracy: 0.75

Data file hash from IPFS: QmeMrshERX7NYXXJE7HCAt8jHY17TeWB1G9y15rskjD1qx
User input data hash: QmeMrshERX7NYXXJE7HCAt8jHY17TeWB1G9y15rskjD1qx
User input source ID: SOURCE1
Block Number: 7
Transaction Count: 1
Transaction successful.
Data ID: QmeMrshERX7NYXXJE7HCAt8jHY17TeWB1G9y15rskjD1qx
Correctly classified count by using Combined approach: 281
Misclassified count by using Combined approach: 19
Accuracy: 0.94
Updated reputation: 0.8004087736789631
```

Fig. 5: CLI Output

III. Conclusions and Future Work

This demonstration presents an approach that integrates machine learning with blockchain to enhance trustworthiness in cold chain logistics. We emphasize that blockchain can not only ensure transparent tracking of goods' conditions throughout the supply chain but also facilitate distributed validation of data accuracy, which is crucial for the reliability of such systems. Moving forward, we plan to investigate other machine learning methods to improve this approach in terms of accuracy and efficiency. We will also explore broader use cases, integrations, and the adaptability of this approach to other contexts and industries.

References

[1] M. Yu, H. Zhang, J. Ma, X. Duan, S. Kang, and J. Li, "Cold chain logistics supervision of agricultural products supported using internet of things technology," *IEEE Internet of Things Journal*, 2024.

[2] R. Ratnayake, M. Liyanage, and L. Murphy, "Evaluating data trust in blockchain-based IoT systems using machine learning techniques," in *IEEE 22nd Consumer Communications & Networking Conference*, 2025.

[3] P. Bodik, W. Hong, C. Guestrin, S. Madden, M. Paskin, and R. Thibaux, "Intel lab data," 2004.

[4] T. Tadj, R. Arablouei, and V. Dedeoglu, "On evaluating IoT data trust via machine learning," *Future Internet*, vol. 15, no. 9, 2023.