Machine Learning for Data Trust Evaluations in Blockchain-Enabled IoT Systems

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*—Recently, there has been a surge of interest surrounding the integration of blockchain with the Internet of Things (IoT), aiming to address IoT's inherent issues like single points of failure and concerns related to data integrity. However, although blockchain provides decentralization and transparency, it does not guarantee the accuracy and reliability of IoT-generated data. Therefore, additional measures are needed to assess and verify the reliability of IoT data stored on blockchains. In this demonstration, we present a novel approach that employs support vector machine (SVM) models in edge servers and multiple machine learning (ML) models executed by validators for data trust evaluations in blockchain-enabled IoT systems. Our approach introduces a composite trust metric that combines past device reputation on the blockchain with real-time data assessment enabled by SVM models. This composite measure provides a dynamic method for determining the trustworthiness of data at the point of submission. The multiple different ML models used by validators work as a distributed ensemble, leading to improved classification accuracy. This novel approach helps to calculate reputation scores more accurately, increasing the system's reliability. We illustrate the feasibility of our approach through a description of our prototype implementation.**

***Index Terms*—Blockchain, IoT, Trust Management, Data Trust Evaluation, Machine Learning, Smart Contracts**

I. Introduction

The integration of blockchain technology with the Internet of Things (IoT) has garnered significant attention in recent years. This convergence is primarily motivated by the distinctive features inherent in blockchain, such as its decentralized ledger, immutable storage, data availability, and transparency. The nature of blockchain's tamper-resistant architecture safeguards against unauthorized modifications, ensuring that once data is added to the ledger, it remains unaltered. However, a critical challenge persists — the inability of blockchain to inherently guarantee the accuracy of the data it holds.

In IoT systems, where data accuracy significantly impacts application and service effectiveness, establishing robust frameworks for data trust evaluation becomes crucial. These frameworks may encompass reputation-based systems, machine learning (ML) algorithms for anomaly detection, and collaborative validation mechanisms. By integrating these methods, blockchain-enabled IoT systems can move beyond the assurance of tamper resistance to ensure that the data within the ledger is secure, accurate and dependable.

Recent research [1], [2] explores the implementation of reputation systems for evaluating trust in IoT data, which are primarily concerned with determining the trustworthiness of devices, taking into account external factors, device relationships, and past data contributions. Although this historical approach is informative, it may not fully capture the reliability of real-time data introduced into the system.

To address this gap, this demonstration introduces a novel approach using ML techniques for reliable data trust evaluations on blockchain-enabled IoT systems.

II. Proposed Solution and Prototype Design

The proposed solution approach involves a sequence of steps, as shown in Fig. 1 and briefly described below.

1) Upload sensor data: IoT sensors upload real-time data to an edge server in a particular neighborhood.
2) Classification by Support Vector Machine (SVM) model: At the edge server, data preprocessing includes cleaning, normalization, and feature engineering. A pretrained SVM model classifies the data as trustworthy or untrustworthy. To counteract edge server misbehavior, the SVM model can be run through blockchain-based smart contracts using a decentralized oracle.
3) Retrieve reputation scores: The edge server retrieves reputation scores (R_s) from InterPlanetary File System (IPFS) for corresponding sensors.
4) Calculate the Composite Trust Score: A Composite Trust Score (C_s) is calculated by integrating sigmoid-scaled decision scores ($\tilde{D_s}$) from SVM classification with R_s. The trust score weight (λ), modeled using a Gaussian curve with its peak value of 1 at the $\tilde{D_s}$ of 0.5, serves to balance the influence of decision and reputation scores.
$$C_s = (1 - \lambda)\tilde{D_s} + \lambda R_s \quad (1)$$
5) Threshold-based trust labeling: Records with C_s exceeding a predefined threshold are labeled 'trustworthy'; those falling below are labeled 'untrustworthy'. Data points close to the decision hyperplane are tagged as 'misclassification-prone.'
6) Upload labeled data to IPFS: Labeled data records with trust assessments are securely stored on IPFS.
7) Upload hashes to the blockchain: Hashes of these records are uploaded to the blockchain for data integrity, transparency, and tamper-resistance.
8) Validator-driven verification: Validators assess the trustworthiness of misclassification-prone data records using their own ML models.
9) Collect validators' votes: Validator assessments are uploaded as votes and collected by a smart contract.
10) Evaluate votes: The smart contract calculates the majority vote, verifies data record labels, and adds new entries with correct labels in case of discrepancies.

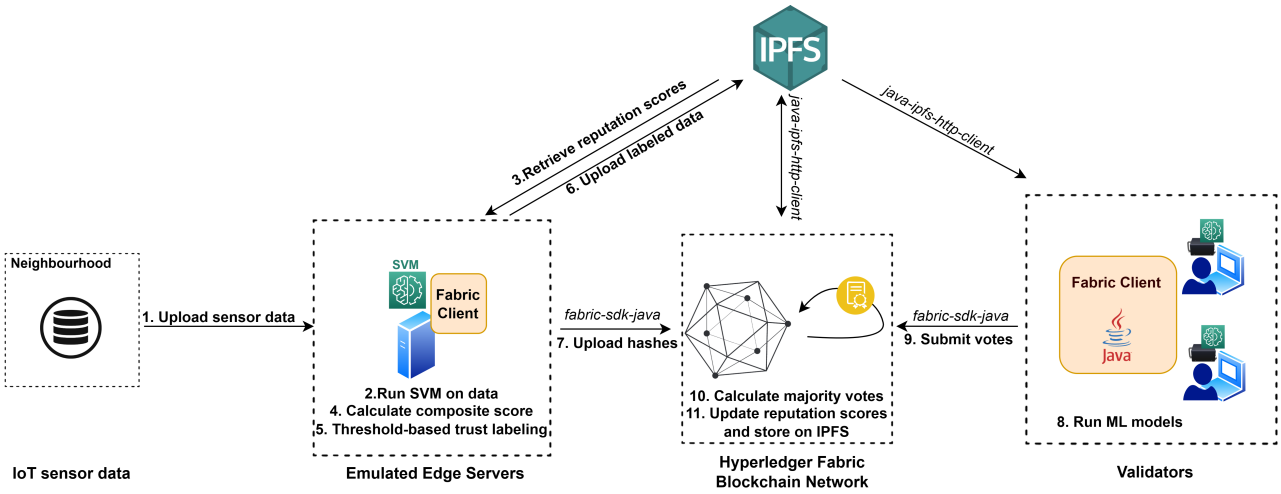

Fig. 1: Overview of the proposed solution and prototype design

11) Update reputation scores: Reputation scores of corresponding sensors are updated by a smart contract using combined predicted labels formed using the SVM classifications for data records with decision scores outside the misclassification-prone range, and the interpretations of validators for data records within the misclassification-prone range. The reputation score is calculated as the ratio of data deemed trustworthy by the system to the total data provided by the sensor. The updated reputation scores are stored in the IPFS.

The prototype, while not a comprehensive end-to-end development, is sufficient to showcase the feasibility of the proposed solution. IPFS provides off-chain storage expanding scalability and facilitating the distribution of large volumes of data with reduced redundancy compared to blockchain systems. The blockchain development was executed using Hyperledger Fabric v2.4 in the Java programming language, with the Raft consensus algorithm being employed. Python was used for the implementation of ML models. A Java application was utilized to simulate edge servers interacting with IPFS and the blockchain, and the validators interacting with the blockchain smart contract.

For our experiments, we utilized temperature readings from 10 sensors extracted from the Intel Lab dataset [3]. To simulate untrustworthy data, we employed the Random Walk Infilling (RWI) algorithm proposed in [4], generating corresponding untrustworthy data for each temperature reading. The dataset underwent meticulous labeling, marking outliers in the original data and those generated using the RWI algorithm as untrustworthy. Trustworthy labels were assigned to the original data that exhibited no outlier characteristics. Techniques such as cleaning, normalization, and feature engineering, as recommended by the authors of the same reference, were applied to the dataset.

In the context of blockchain-based validation, three distinct models—Multilayer Perceptron (MLP), Random Forest, and K-Nearest Neighbors—were employed by validators. Votes from validators were collected for each data record undergoing validation. The final evaluation by validators was determined through a majority vote mechanism facilitated by a smart contract on the blockchain.

Our results achieve above 90% accuracy in distinguishing trustworthy and untrustworthy IoT sensor data across malicious concentrations ranging from 10% to 90%, outperforming existing SVM-based and MLP-based approaches whose accuracy varied between 75% and 85% in these tests.

III. Conclusions and Future Work

In this paper, we proposed a novel approach to assess trustworthiness of data in blockchain-enabled IoT systems by using ML techniques and demonstrated its feasibility by describing a prototype design. The solution introduced a composite trust metric that combines blockchain-based past reputation with real-time SVM-assisted data assessment. This metric offers better data trust assessment at the point of submission. Multiple ML models on the blockchain enhance the accuracy, acting as a distributed ensemble, for more precise reputation score calculations and increased system reliability. In the future, we plan to extend this work by conducting analyses on additional ML-based solutions to enhance the overall data trust assessment.

Acknowledgement

This work is partly supported by the European Commission under CONFIDENTIAL-6G (Grant:101096435) and SFI under CONNECT P2 (Grant no. 13/RC/2077_P2) projects.

References

[1] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, "A blockchain-based trust and reputation model with dynamic evaluation mechanism for iot," *Computer Networks*, vol. 218, p. 109404, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622004388

[2] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, "Blockchain based trust management mechanism for iot," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–8.

[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. [Online]. Available: https://www.mdpi.com/1999-5903/15/9/309