Green University of Bangladesh

Dept. of Computer Science and Engineering

Final Year Capstone Project/Thesis Proposal Form

Semester: Spring 2023 **Year: 2023** **Course Code: CSE 400A**

Student Information:

Sl.	Id	Name	Email	Cell
1.	201002182	Md. Soikat Hossain	soikatkhan61@gmail.com	01722726897
2.	201002183	Md. Golam Mostafa	gmnayeem25@gmail.com	01303110760
3.	201002093	Obaydullah Khan	obaydullahkhaan@gmail.com	01791423784

Tick (√) the appropriate box: ☐ **Capstone Project** ☐ **Capstone Thesis** ☐ **Project** √ **Thesis**

Proposed Title: Enhancing Traffic Flow Prediction through Blockchain-based Federated Learning with Privacy Protection

Brief Description of the project/thesis: (Extra pages can be used if necessary**)**

Problem Statement and Motivation:

Traffic flow prediction is essential for managing traffic, but current methods for predicting traffic flow using machine learning require gathering raw data, which can put people's privacy at risk. To solve this issue, a new method called federated learning has been introduced. It allows sharing model updates without exchanging raw data, which makes it more secure. However, there are still security challenges with the current federated learning frameworks, which have a central point of control. To address this issue, a new framework based on consortium blockchain has been proposed. This framework is decentralized, reliable, and secure. It uses a differential privacy method to add noise to the model updates, protecting privacy. This new approach can prevent data poisoning attacks and improve the privacy of model updates, making traffic flow prediction more secure.

Literature work and limitation:

1.Limited data diversity: Since the FL participants are selected based on their data relevance,there is a possibility of limited data diversity. This may result in biased training and prediction models, leading to inaccurate results.

2. Communication and computation overhead: The implementation of FL in a blockchain environment requires significant communication and computation overhead. This may lead to increased network latency, higher energy consumption, and reduced system scalability.

3. Security risks: The proposed approach relies on the security of the blockchain network, and any potential security threats to the blockchain may compromise the privacy and security of the FL participants' data.

4. Dependence on a trusted third party: The proposed approach requires a trusted third party (TTP) for the selection and verification of FL participants. The TTP's reliability and integrity are crucial to the success of the FL process, and any compromise to the TTP's security may result in a failure of the FL process.

5. Limited applicability: The proposed approach may not be applicable to all scenarios, such as situations where the FL participants are unwilling to share their data or where there is a lack of participants with relevant data.

Objectives of the project/thesis:

1.Develop a privacy-preserving federated learning framework for traffic flow prediction using blockchain technology.

2. Investigate the effectiveness of the proposed framework in terms of prediction accuracy and model convergence compared to traditional federated learning approaches.

3. Evaluate the privacy preservation capabilities of the proposed framework in terms of protecting the data privacy of participants.

4. Design a consensus algorithm for the consortium blockchain to defend against security attacks launched by malicious entities.

5. Explore the feasibility of the proposed framework in a real-world scenario by conducting experiments using real traffic data.

Project/Thesis Work Methodology:

Data collection: Raw traffic flow data is collected from distributed vehicles, without compromising the privacy of drivers and passengers.

Federated learning: A federated learning approach is used to train a traffic flow prediction model without exchanging raw data. Model updates are shared among the vehicles, and each vehicle uses its own local data to improve the model.

Consortium blockchain: A consortium blockchain is used to store and validate the model updates. Miners verify the validity of each update to prevent unreliable model updates.

Differential privacy: To protect the privacy of model updates on the blockchain, a differential privacy method with a noise-adding mechanism is applied. This adds random noise to the updates to prevent the disclosure of sensitive information.

Evaluation: The effectiveness of the proposed framework is evaluated using numerical simulations. The framework's ability to prevent data poisoning attacks and improve the privacy of model updates is assessed. The performance of the traffic flow prediction model is also evaluated.

Comparison: The proposed framework is compared to existing centralized and decentralized federated learning approaches. The comparison includes factors such as accuracy, privacy, and security.

Student Signature:

1. Soikat
2. Golam Mostafa
3. Obaydullah

Proposed Supervisor: