World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:18, No:02, 2024

Enhancing Robustness in Federated Learning through Decentralized Oracle Consensus and Adaptive Evaluation

Authors : Peiming Li

Abstract : This paper presents an innovative blockchain-based approach to enhance the reliability and efficiency of federated learning systems. By integrating a decentralized oracle consensus mechanism into the federated learning framework, we address key challenges of data and model integrity. Our approach utilizes a network of redundant oracles, functioning as independent validators within an epoch-based training system in the federated learning model. In federated learning, data is decentralized, residing on various participants' devices. This scenario often leads to concerns about data integrity and model quality. Our solution employs blockchain technology to establish a transparent and tamper-proof environment, ensuring secure data sharing and aggregation. The decentralized oracles, a concept borrowed from blockchain systems, act as unbiased validators. They assess the contributions of each participant using a Hidden Markov Model (HMM), which is crucial for evaluating the consistency of participant inputs and safeguarding against model poisoning and malicious activities. Our methodology's distinct feature is its epoch-based training. An epoch here refers to a specific training phase where data is updated and assessed for quality and relevance. The redundant oracles work in concert to validate data updates during these epochs, enhancing the system's resilience to security threats and data corruption. The effectiveness of this system was tested using the Mnist dataset, a standard in machine learning for benchmarking. Results demonstrate that our blockchain-oriented federated learning approach significantly boosts system resilience, addressing the common challenges of federated environments. This paper aims to make these advanced concepts accessible, even to those with a limited background in blockchain or federated learning. We provide a foundational understanding of how blockchain technology can revolutionize data integrity in decentralized systems and explain the role of oracles in maintaining model accuracy and reliability.

Keywords : federated learning system, block chain, decentralized oracles, hidden markov model
Conference Title : ICSTSSS 2024 : International Conference on Systems Theory, Systems, Subsystems and Supersystems
Conference Location : Rome, Italy
Conference Dates : February 19-20, 2024