

Blockchain for AI Model Verification: Ensuring Transparency in AI Training Data

Mr. Aniket Shekhar Boghum and Dr. Abhijit Banubakode

MET Institute of Computer Science, Mumbai, India

mca23_1410ics@met.edu

Abstract: Artificial Intelligence (AI) technologies are becoming more entrenched in important domains like finance, healthcare, and the government. The integrity and ethical soundness of such systems rely almost entirely on the transparency and quality of their training data. Unfortunately, existing AI training cycles seldom have strong enough mechanisms in place to ensure data provenance and integrity, with the result that there is risk of bias and exposure. This work discusses blockchain integration as a solution to authentication and ensuring the transparency of AI training datasets. Through the decentralized and immutable ledger of blockchain, we introduce a framework that documents the provenance of training data, allowing for traceability and minimizing the chance of data tampering. Smart contracts are deployed to automate the process of validating data and verifying compliance with defined ethical standards. Our results indicate that the integration of blockchain can considerably increase the credibility of AI models by offering an open and immutable record of training data, thus ensuring increased accountability and reliability in AI-based decision-making processes. The inclusion of privacy-enhancing technologies like zero-knowledge proofs (ZKPs) and formal verification techniques further enhances the framework, enabling it to be used in sensitive applications..

Keywords: Blockchain, AI Verification, Data Transparency, Smart Contracts, Bias Detection, Zero-Knowledge Proofs

