ABSTRACT

In the digital era, smartphones are pivotal for documenting life events, frequently providing critical evidence in judicial proceedings. Yet, the dispersion of this digital evidence across a multitude of devices, coupled with its dissemination through social media, poses a significant challenge for law enforcement agencies. The complexities of aggregating and scrutinizing such data are compounded by the computational demands of extracting and preserving relevant media. Additionally, the advent of deepfake technology has introduced sophisticated methods for disseminating misinformation, enabling harassment and manipulation that threaten the integrity of digital evidence.

This dissertation introduces the Blockchain-Based Decentralized Federated Learning Framework for Digital Forensic Applications & Deepfake Detection (BFDD), a powerful tool specifically designed to aid law enforcement agencies in authenticating digital evidence. The designed Decentralized Application (Dapp) leverages a decentralized, federated learning framework to streamline targeted data extraction and enhance the detection of deepfakes using machine learning, thereby equipping digital forensic investigators with a robust tool for evidence verification. This application is developed to address the growing challenges in digital forensics brought about by generative AI and the proliferation of deepfakes. It seeks to enhance evidence authentication techniques, thereby reinforcing the reliability of digital media in legal settings.

Keywords: Digital Forensics, Federated Learning, Blockchain, Deepfake, Machine Learning