Paper 1

Blockchain Based Approach for tackling Deepfake videos Ujwal Patil1, Prof. P. M. Chouragade2 1M.Tech ,Computer Science and Engineering, GCOE, Amravati, Maharashtra, India 2Assistant Professor, Computer Science and Engineering, GCOE, Amravati, Maharashtra, India

Summary

1. **Video Creation and Storage**:
    - The original artist (owner) registers on the IPFS.
    - The video, along with its metadata, is uploaded to the IPFS.
    - IPFS generates a unique hash for the video, which is then stored on the Blockchain.
2. **Video Verification**:
    - When a user retrieves a video from IPFS and posts it on social media, a verification process is initiated.
    - The system compares the hash of the uploaded video with the original hash stored on the Blockchain.
    - If the hashes match, the video is considered authentic. If they do not match, the video is flagged as potentially manipulated or fake, and the user's trust factor is adjusted accordingly.

Limitations

- **Reliance on the Original Creator**: The entire system assumes that the original creator (owner) is trustworthy. If the original video itself is a deepfake or manipulated, the system will not detect it, and the false content will be verified as authentic.
- **Time-Consuming Verification**: Retrieving videos from IPFS and verifying them against Blockchain records can take time, which might not be practical for real-time verification, especially in scenarios where immediate action is needed

Paper 2

Journal of Korea Multimedia Society Vol. 24, No. 8, August 2021(pp. 1044-1058) https://doi.org/10.9717/kmms.2021.24.8.1044 Blockchain Technology for Combating Deepfake and Protect Video/Image Integrity Md Mamunur Rashid†, Suk-Hwan Lee††, Ki-Ryong Kwon†††

Summary

The framework uses blockchain to create a decentralized, tamper proof system for sharing digital content (like videos and images).The system employs smart contracts to manage and secure video content. A smart contract is triggered when a video is uploaded, generating a hash that includes critical metadata. The contract governs who can access or edit the video, enforcing permissions and ensuring the content's integrity.

When a user uploads or downloads a video, the Dapp communicates with the smart contract to authenticate the transaction. The video's value is deducted from the downloader's balance (in Ether) and transferred to the owner. The smart contract then updates the permissions accordingly. The framework makes it easy to verify the authenticity of a video, as any changes are logged on the blockchain.

Limitations

High Costs: The use of blockchain, particularly for storing and processing large amounts of data, can be expensive. Transaction fees (e.g., gas fees on Ethereum) can add up, making it costly to upload, manage, and validate digital content.

Storage Limitations: Blockchains are not designed for storing large files like videos.

Paper 3

Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain Bela Gipp University of Konstanz, bela.gipp@uni-konstanz.de Jagrut Kosti University of Konstanz, jagrut.kosti@uni-konstanz.de Corinna Breitinger University of Konstanz, corinna.breitinger@uni-konstanz.de

Summary

The system described is an Android application that records dashcam video using the phone's camera while driving. It continuously records short video segments, which are stored temporarily and overwritten if no collision occurs. When a collision is detected using the phone's accelerometer, the app saves the relevant video segments (before, during, and after the impact) and computes a SHA-256 hash of the combined video file. This hash is then sent to the OriginStamp service, which stores it in the Bitcoin blockchain. This process ensures that the video file's integrity is maintained and any tampering can be detected.The app runs in the background, even when other applications are in use, and displays a small video feed on the screen. If a collision is detected, the app also notifies the user's emergency contacts with the collision location. The system allows users to manually save and timestamp video recordings for other significant events. Finally, the application provides a way to verify the video file's integrity by comparing the hash with the one stored in the blockchain, ensuring the video hasn't been altered since its timestamping.

Limitations

Submission Delay: Hashes are submitted to the Bitcoin blockchain with a 24-hour delay due to cost-saving measures. Immediate submission could improve timestamp accuracy.

Bitcoin Dependency: The system's reliance on Bitcoin may lead to higher costs due to potential fee increases. Alternatives like Ethereum could reduce costs but might lack Bitcoin's trustworthiness.