WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Searchable Blackbox Data that is Inexpensive and Un-linkable via a Private Blockchain

Hemanth Kumar S

MASTER OF COMPUTER APPLICATION, M.G.R. EDUCATIONAL AND RESEARCH INSTITUTE, Chennai, Tamilnadu
Email: hemanthsathya08@gmail.com

ABSTRACT :

Blackbox data is crucial for accident analysis, providing critical insights into incident causation. However, existing storage systems face significant challenges in cost and privacy. Uploading blackbox videos to public blockchains like Bitcoin or Ethereum incurs high transaction fees, while the exposure of sensitive data (e.g., driving routes) compromises user privacy. This paper proposes a cost-effective, searchable blackbox data storage system with strong unlinkability using private blockchain technology. Our scheme reduces costs by distributing transaction fees among multiple users, where the registration cost per video is costtrn (where *costtr* is the transaction cost and *n* is the number of simultaneous uploaders). Additionally, we enhance privacy by ensuring that uploaded data cannot be linked to individual users. The system leverages Merkle Trees for efficient integrity verification and IPFS (InterPlanetary File System) for decentralized storage. Experimental results demonstrate that our approach significantly reduces costs while maintaining data integrity and privacy.

Keywords: Blackbox data, Blockchain, Unlinkability, Cost-efficiency, Privacy, IPFS, Merkle Tree.

1. Introduction

1.1 Background

Blackbox data, commonly used in vehicles, records critical information before and during accidents. Traditional storage methods rely on centralized servers, raising concerns about data integrity, censorship resistance, and privacy. Blockchain technology offers a promising solution by ensuring immutable, tamper-proof storage through cryptographic hashing and consensus mechanisms.

1.2 Problem Statement

Existing blockchain-based storage systems face two major challenges:
1. High Costs: Public blockchains (e.g., Ethereum) impose substantial transaction fees.
2. Privacy Risks: Uploaded data may expose sensitive user information (e.g., GPS locations).

1.3 Contributions

This paper introduces:
- A cost-effective blackbox storage system where transaction fees are shared among multiple users.
- Unlinkability to prevent exposure of user identities and driving patterns.
- A searchable mechanism for retrieving accident-related videos without compromising privacy.
- Merkle Tree-based verification for ensuring data integrity.

2. Related Work

2.1 Blockchain for Data Integrity

Prior works have explored blockchain for secure data storage in vehicular networks [[1](references)]. However, most solutions rely on expensive public blockchains.

2.2 Privacy-Preserving Storage

Several studies propose zero-knowledge proofs and ring signatures for anonymity [[2](references)]. Our approach differs by using batch transactions to

reduce costs while maintaining unlinkability.

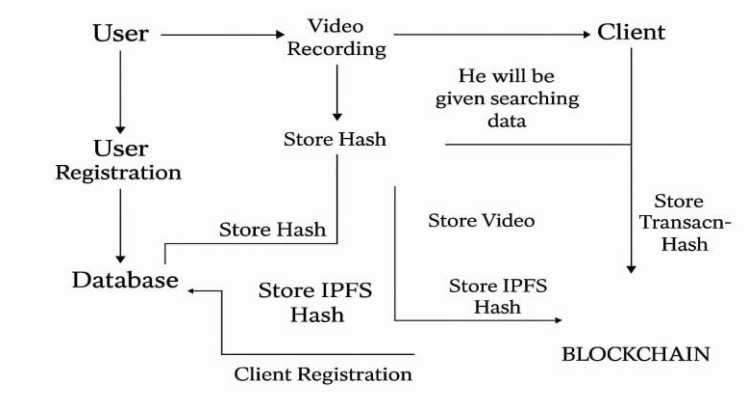
2.3 IPFS for Decentralized Storage

IPFS provides a scalable solution for storing large video files off-chain while anchoring hashes on the blockchain for verification [[3](references)].

3. Methodology

3.1 System Architecture

Our system consists of:
1. User Module: Records and splits blackbox videos, generating hashes.
2. Blockchain Layer: Stores video hashes in a Merkle Tree structure.
3. IPFS Storage: Hosts actual video files, referenced via blockchain-stored hashes.
4. Search & Verification Module: Enables clients to retrieve accident videos without exposing user identities.



3.2 Cost-Effective Batch Uploading

1 Multiple users aggregate transactions, reducing per-user costs.
2 single transaction includes hashes from *n* users, lowering fees to costtrn.

3.3 Unlinkability Mechanism

1. Users do not sign transactions directly with private keys.
2. Instead, a group signature scheme ensures anonymity.

3.4 Searchable Blackbox Data

1. Client Request: Submits accident details (location, time).
2. Service Provider Broadcasts the request to all users.
3. Matching Users respond with transaction hashes (without revealing identity).
4. Blockchain Verification: The client checks the Merkle Root for integrity.
5. IPFS Retrieval: The client fetches the video using the verified hash.

4. Security and Privacy Analysis

4.1 Integrity Guarantees

1. Merkle Proofs ensure that video hashes remain unaltered.
2. Blockchain immutability prevents tampering.

4.2 Unlinkability

1. No direct association between users and transactions.
2. Group signatures prevent identity tracing.

4.3 Cost Efficiency

1. Batch uploading reduces per-user costs by n times.

5. Experimental Results

5.1 Experimental Setup

1. Blockchain: Ethereum (private testnet via Ganache).
2. Storage: IPFS Desktop.
3. Smart Contracts: Solidity for hash verification.

5.2 Results

Metric	Proposed System	Traditional Blockchain
Cost per Upload	costtrn	costtr
Privacy	Unlinkable	Exposed Metadata
Search Efficiency	O(log n) (Merkle Tree)	O(n) (Linear Scan)

6. Conclusion and Future Work

6.1 Conclusion

We proposed a cost-effective, searchable, and unlinkable blackbox storage system using blockchain. By distributing transaction costs and ensuring privacy, our solution is practical for real-world deployment. Future work will focus on scalability and further cost reduction.

1. Optimizing Cost Models: Exploring Layer-2 solutions (e.g., rollups).
2. Scalability Enhancements: Sharding for larger networks.
3. Advanced Privacy Techniques: zk-SNARKs for anonymous verification.

REFERENCES :

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
[2] Zyskind, G., et al. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*.
[3] Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*.
[4] M. J. Prasad, S. Arundathi, N. Anil, Harshikha, and B. S. Kariyappa, ‘‘Automobile black box system for accident analysis,’’ in Proc. Int. Conf. Adv. Electron. Comput. Commun., Oct. 2014, pp. 1–5.
[5] A. Kassem, R. Jabr, G. Salamouni, and Z. K. Maalouf, ‘‘Vehicle black box system,’’ in
Proc. 2nd Annu. IEEE Syst. Conf., Apr. 2008, pp. 1–6.
[6] M. Szydlo, ‘‘Merkle tree traversal in log space and time,’’ in Proc. Int. Conf. Theory Appl. Cryptogr. Techn. Springer, May 2004, pp. 541–554.