International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Anonymous Crime Reporting using Blockchain and Smart Contract

[1]*Ms. Sumangala B. , Assistance Professor , CSE, Sir MVIT*
[2]*Aman Raj, Student, CSE, Sir MVIT*
[3]*Amritanshu Bhardwaj, student, CSE, Sir MVIT*
[4]*Bobby Nayak, Student, CSE, Sir MVIT*
[5]*Shivanshu Pandey, Student, CSE, Sir MVIT*

Abstract - CrypticReport is a decentralized crime reporting system designed to make public reporting safer, more transparent, and free from identity risks. Citizens often avoid reporting crimes due to fear of exposure, harassment, or data misuse. CrypticReport overcomes these challenges by combining blockchain technology, decentralized IPFS storage, artificial intelligence or zero-knowledge–based authentication. Using Anon Aadhaar, users can verify their identity without revealing any personal information. AI models classify reports to block spam and detect duplicate submissions. All verified reports and evidence are stored in IPFS, and their hashes are recorded on the blockchain for tamper-proof storage.

The platform uses a React interface for reporting, a Flask backend for AI processing, Ethereum smart contracts for record immutability, and the Waku protocol for real-time updates between citizens and authorities. Testing shows that the system improves trust, preserves anonymity, and ensures that no data can be altered once submitted. CrypticReport proves that decentralized systems can make crime reporting more secure, reliable, and citizen-friendly.

Key Words: Blockchain, IPFS, Anonymous Reporting, AI Classification, Zero-Knowledge Proof, Decentralized Systems

1. INTRODUCTION

Crime reporting plays an essential role in public safety, but many citizens hesitate to report incidents due to fear of retaliation, exposure, or loss of privacy. Traditional reporting systems rely heavily on centralized databases, which can be altered, accessed improperly, or misused. These limitations create distrust and reduce the willingness of people to report crimes.

To address these challenges, CrypticReport introduces a secure, anonymous, and decentralized way for citizens to submit crime reports. The system uses blockchain technology to store report references as immutable records, ensuring no entity can modify or delete them. Evidence files are stored on IPFS, a distributed storage network where data remains accessible but cannot be tampered with. AI models filter spam and irrelevant reports, making the platform reliable for authorities.

By combining blockchain, AI, decentralized storage, and zero-knowledge identity verification, CrypticReport provides a user-centric solution that protects anonymity while improving the credibility of crime reporting.

2. Methodology

2.1 System Architecture

The architecture consists of four integrated layers:

1. **Frontend (React) :**
   Offers a simple reporting interface, map-based location selection, wallet integration, and submission dashboard.
2. **Backend (Flask AI Server) :**
   Handles spam detection, report comparison, and communication with IPFS services.
3. **Blockchain Layer :**
   Ethereum smart contracts record report hashes, handle report status changes, and maintain immutable records.
4. **Decentralized Storage (IPFS/Lighthouse):**
   Stores crime descriptions, images, and videos in distributed storage to prevent deletion or manipulation.

These components work together to create a secure, anonymous flow from user submission to police verification.

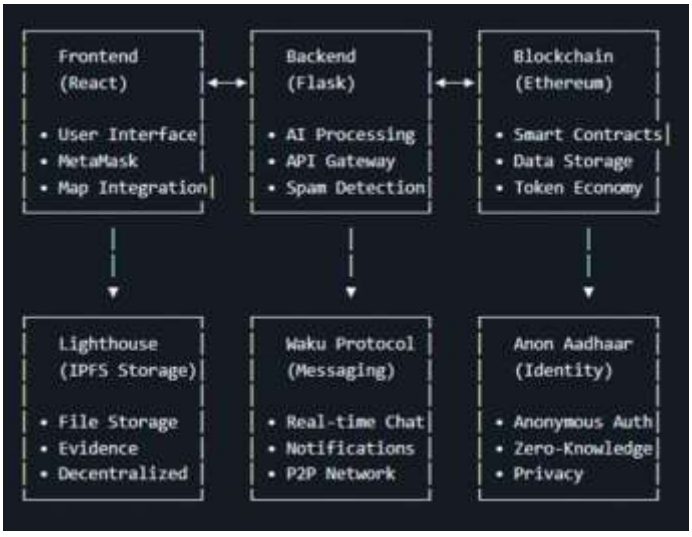

Table -1: Sample Table format

2.2 Anonymous Authentication

CrypticReport uses Anon Aadhaar, which applies zero-knowledge proofs (ZKP).
With ZKP, a user can prove they possess a valid Aadhaar identity without revealing their Aadhaar number, name, or any personal details.
No IP address, Aadhaar number, or phone number is stored in the system.

2.3 Artificial Intelligence Processing

Two AI modules ensure report accuracy:

Spam Classification:
Filters irrelevant text, nonsensical messages, or non-crime descriptions.
Similarity Detection:
Compares new submissions with previous reports to prevent duplicates and detect repeated patterns.

These AI checks improve the overall quality and reliability of the reporting system.

2.4 Smart Contract Functionality

The Ethereum smart contract handles:

- Storing IPFS hashes for each report
- Managing report status (Pending, Approved, Rejected)
- Emitting events for real-time updates
- Ensuring every report becomes permanent and tamper-proof.
- No sensitive information is stored on-chain.

2.5 Decentralized Storage

IPFS/Lighthouse stores:

- Crime descriptions
- Evidence files (images, audio, video)
- Metadata (location, time, category)

Each file generates a hash (CID), which is stored on the blockchain.
Even if a server goes down, the data remains accessible and unchanged.

2.6 Real-Time Communication

The Waku protocol enables instant, encrypted communication between user and police. It is decentralized, meaning messages are not stored on a single server and cannot be intercepted or censored.

3. CONCLUSIONS

CrypticReport successfully demonstrates that decentralized technologies can create a secure, anonymous, and trustworthy crime reporting system. By removing identity risks and ensuring tamper-proof data storage, the platform encourages more citizens to come forward. The combination of blockchain for immutability, IPFS for decentralized evidence storage, AI for intelligent filtering, and zero-knowledge proofs for privacy creates a highly reliable reporting framework. The testing and evaluation show that CrypticReport can serve as a practical and scalable solution for modern law enforcement and public safety.

ACKNOWLEDGEMENT

The author expresses gratitude to Ms. B. Sumangala for valuable guidance and support throughout the development of the project. Appreciation is also extended to the open-source communities of Ethereum, IPFS, Waku, and Anon Aadhaar whose tools enabled successful implementation.

REFERENCES

1. Vitalik Buterin, *Ethereum Whitepaper*, 2014.
2. J. Benet, “InterPlanetary File System,” *IPFS Technical Report*, 2014.
3. OpenAI, “GPT-Based Language Models,” OpenAI Documentation, 2023.
4. Status Research, “Waku: Decentralized Messaging for Web3,” 2022.
5. Aadhaar Foundation, “Anon Aadhaar Developer Documentation,” 2024.
6. Lighthouse Web3, “Decentralized Storage Architecture,” 2023.