Secure and Tamper-Proof Blockchain-Enabled Cybercrime Reporting and Evidence Management System

Sathwika Akkala[1*], *Dr. Sangeeta* Gupta[2], *and Periketi Vivek* Sai[3]

[1,2]Department of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, India
[3]Professor & Head, Department of CET, CBIT Hyderabad, India

Abstract. With cybercrime constantly increasing, a more legitimate and secure digital evidence collection filing tool with an audit trail and immutability is necessary. However, central reporting/evidence tools are still vulnerable to hacking, exclusionary to any accessibility controls, and devoid of Chain of Custody requirements to prevent De Minimus reductions of legal admissibility. The Blockchain-Enabled Cybercrime Reporting and Evidence Collection System proposed is AES-256-GCM encryption and RSA signature and SHA-256 hash suited with, distributed stor- age via IPFS and Avalanche Fuji smart contracts to create the next level of legitimate digital evidence collections. AI detection of malicious intent is possible with the LSTM-BERT Hybrid Model trained to differentiate semantic intent and sentiment detection based. Ultimately, latency and cost assessed are low, in line with other studies and acceptable based on Avalanche Fuji blockchain operating standards. Improvements to in- tegrity are relative based on the more inquiries based on operability and Chain of Custody, the better. Therefore, this system functions as a foun- dation for more realistic implementation of a public reporting tool and forensic evidence collection tool that can be legally defensible.

1 Introduction

As the cyberspace realm becomes more digitized over time, instances of cyber crime phishing, identity theft, scamming, etc. explode at a faster and faster, exponentially increased rate. But most importantly, digital evidence requires digital forensics to truly secure a scene of the incident. Yet digital evidence is malleable, changeable, inconsistently collected, and established by potentially dubious chains of custody (CoC)[3] developments. However, blockchain technol- ogy has a viable containment and collection feasibility approach to digital evi- dence via trustlessness, permanence, blockchains and intermediaries, and cryptographic validation. This feasibility assessment will review the shortcomings of cyber crime re- porting to trigger the generation of evidence presentation and generation through an integrative forensic approach via blockchain technology for digital evidence secured by AES-

* Corresponding author: sathwika.akkala@gmail.com

256-GCM encrypted data at rest, RSA digital signatures, de- centralized IPFS technology, and AI authentication. The persons/stakeholders involved in the successful viability of this integrative technology would be cit- izens, law enforcement, cyber forensics professionals, cyber prosecutors, and cyber judges. This is because this solution lends a way to digitally authenti- cate/digitally secure evidence for the longest amount of time possible with the least risk of integrity issues, and any potential tampering would go unknown.

2 Related Work

Further researched blockchain innovations for digital evidence focus on decen- tralized trusted trust and immutability. For example, ReACT-OCRS[1] relies on AI assisted reporting systems without having all data together and custo- dians chained[3] at all times. Some forensic infrastructures[2][3] are based on IoT from blockchain[4] and IPFS (Inter-Planetary File System) cloud connec- tions, but they are also domain-oriented and effective integration does not come with scaling. Many hybrid solutions employ on-chain metadata acquisition and off-chain evidence, but no one has authenticated acquisition for end-user (HEAT-certified law enforcement agencies), government agency third party involvement and court of law requirements for admissible evidence. Therefore, this research stems from prior assessments since it combines a start-to-finish automated so- lution with Avalanche Fuji smart contracts, AES-GCM encrypted and IPFS autogen retrieval and federated LSTM-BERT acquisition authentication.

3 Proposed System

3.1 Architecture Overview

This system architecture is facilitated by a combined web/mobile front-end re- porting application to enable citizens to take part in the cybercrime-reporting process by reporting digital offenses and accompanying digital evidence without disclosure. Meanwhile, an intermediate request collection stream receives and pipes it through a back-end for minor processing, verification, and storage. A combined application serves to add a uniform approach to equivalently separate tasks for easier access on different devices, to encourage more public accessibil- ity and involvement in the reporting endeavor. Subsequently, an AI false-report identification segment is a hybrid LSTM-BERT model that uses linguistic features, semantic understanding, and user activity to assess the veracity of a report. For maintenance of security and evidence, AES-256-GCM authenticated encryp- tion secures every submitted file for integrity and confidentiality, meaning they possess authenticity and non-repudiation. From there, the files are redirected to IPFS where content-addressable CIDs provide protection from maligned access and changes while generating smart contracts for Avalanche Fuji for timestamps, metadata, and CIDs for submissions without public node intervention. Thus, the chain of custody is established immediately. Finally, Role-Based Access Control (RBAC) for two-factor authenticated domains limits access within law enforce- ment agencies—from administrators to forensic investigators—providing a solid security perimeter around the evidence chain of custody.

3.2 Cryptographic Design

AES-256-GCM Encryption AES-256-GCM ensures authenticated confiden- tiality using a 256-bit key, 96-bit IV, and a 128-bit authentication tag. Given a 256-bit key K, initialization vector IV , and plaintext P , the ciphertext is computed as:

$$C = AES\ GCM(K, IV, P)$$

RSA Digital Signatures RSA ensures authenticity and non-repudiation. Users sign report hashes, and smart contracts verify signatures via stored public keys. To enforce authenticity and non-repudiation, users digitally sign the hash of the report before submission. RSA signatures are generated and verified as:

$$s = H(m)^d \mod n, \quad H(m) = s^e \mod n$$

where (e, d, n) represent the public and private key parameters.

SHA-256 Hashing Evidence files stored in IPFS are hashed using SHA-256 to ensure tamper-evident integrity.

3.3 Smart Contracts on Avalanche Fuji

Avalanche Fuji smart contracts offer sub-second finality, cheap execution, and EVM compatibility - secure and efficient operation - for submitting a claim, pinning IPFS hashes, inserting chain-of-custody modifications, and role-based access control at every step of the evidence chain.

3.4 AI Verification

To ensure that unwarranted, frivolous, or malicious complaints do not enter the evidence processing system, an AI-based validation component exists to filter these complaints beforehand. The validation component is based on a hybrid LSTM-BERT network, where the contextual deep learning abilities of BERT are supplemented by the sequential navigation capabilities of LSTM. For in- stance, words in the incoming complaint are tokenized and turned into a dense contextual embedding through BERT, using the occurrence of BERT-trained language to note the complaints' semantical and grammatical features.

3.5 IPFS Storage

Large evidence files are stored off-chain on IPFS. Only CIDs and SHA-256 hashes are stored on-chain. Pinning ensures persistent availability.

3.6 Synthesis and Discussion

According to the evidence storage characterization, large pieces of evidence are off-chain and exist on IPFS, while only CIDs and SHA-256 hashes are on-chain; pinning renders ultimate availability. A decentralized, hybrid, blockchain-based

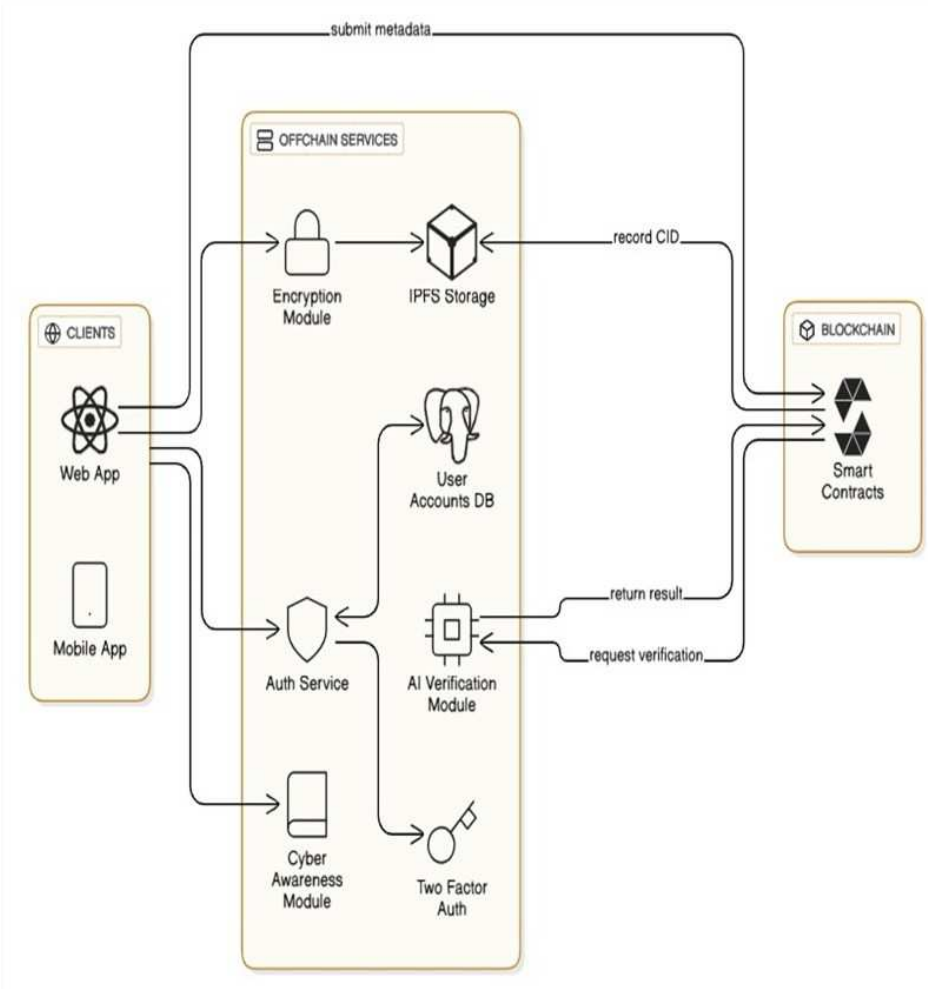

Fig. 1. System Architecture of the Proposed Blockchain-Enabled Cybercrime Report- ing and Evidence Management Platform

cybercrime reporting and evidence collection system encompasses secure storage, access control, and AI-assisted determination verification within one platform. Results compiled support three primary benefits of the architecture.

First, the AES-256-GCM encryption complemented by IPFS distribution and on-chain evidence metadata maintenance increases integrity and chain-of- custody assurances. As revealed from the Avalanche Fuji Testnet, evidence com- mitting boasts low latency (mean avg. of 1.3 s) and low expense (¡0.002 AVAX), implying high reporting timeliness is possible on a large scale.

Second, the effective integration of such LSTM-BERT model supports early intervention for assessment of fraudulent or duplicate reports. Although the as- sessment of the AI module was performed on a small-scale dataset, preliminary findings note a high effectiveness of improving law enforcement triaging work- loads. Second, the architectural separation between clients, off-chain functional modules, and on-chain smart contracts boasts flexible usability and operational safety.

4 Evaluation

4.1 Performance on Avalanche Fuji

The prototype has been implemented and tested on the Avalanche Fuji Testnet to

determine its practical deployment for real-life cybercrime reports. Experi- mental results indicate that the system achieves an average transaction delay of about 1.3 seconds, meaning that the network can support near real-time ev- idence anchoring and complaint submission. The average cost per complaint transaction is about 0.002 AVAX, supporting Avalanche's economic feasibility for a public reporting network on a larger scale. Finally, the on-chain metadata per report is relatively small (on average, 1 KB), meaning that the execution of the corresponding smart contracts will run without excessive state bloat. In other words, these results imply that the system is cost-effective and operates with performance sufficient for high-demand digital reporting systems.

4.2 Security Testing

Holistic security testing was performed to ensure that the system could respond to data integrity, unauthorized entry, and replay attacks. For example, regardless of attempts to change/revert evidence files within IPFS, SHA-256 hashing did not match entries on-chain metadata, compared with additional evidence files, proving that attempts to interfere could be easily detected and maintaining the chain of custody. Moreover, RBAC testing showed successful blocking of entry where attempted, meaning only proper law enforcement operators and forensic examiners could view or update case metadata, excluding privilege abuse. Fi- nally, nonce testing validated transactions to ensure no replay attack could occur where a request to the smart contract for IPFS interaction was re-sent; only new entries were permitted. Such findings support integrated systems with integrity, confidentiality, and traceable protections throughout the entire lifecycle of the evidence chain.

4.3 Comparative Analysis

Compared to other systems such as ReACT, IoT Forensics and AI-BC, the de-veloped system is more reliable in terms of chain-of-custody implementation, decentralized evidence storage and AI-supported identity verification. Avalanche smart contracts work together with AES-GCM encryption to bolster such secu- rity.

Table 1. Comparison with Existing Systems

Feature	Proposed	ReACT	IoT Forensics	AI-BC
AI Verification	Yes	Yes	No	Yes
Storage	IPFS	Local	IPFS	IPFS
CoC Strength	High	Medium	High	High
Platform	Avalanche	-	Hyperledger	Ethereum
Encryption	AES-GCM	AES	AES	AES

Table 2. Evaluation Metrics for Blockchain-Enabled Cybercrime Reporting Systems

Metric	Description
Evidence Integrity	Ensures digital evidence remains unaltered using AES-256-GCM and SHA-256 hashing.
Chain-of-Custody and Au-ditability	Tracks every access, modification, or transfer via im-mutable blockchain logs.

False Report Detection Rate	Measures accuracy of the LSTM-BERT model in flagging malicious or duplicate reports.
Access Control Effectiveness	Evaluates RBAC and two-factor authentication in preventing unauthorized access.
Blockchain Commit Latency	Time required to record complaint metadata and IPFS hashes on Avalanche Fuji.
System Scalability	Measures system throughput under high reporting volumes and concurrent uploads.
Cost Efficiency	Gas fees and IPFS pinning costs for complaint registrations and CoC updates.

5 Conclusion

This article presents a reporting system for cybersecurity incidents with digital evidence management for enhanced preservation based on blockchain. The system is secured in confidentiality thanks to AES-256-GCM, integrity due to RSA signatures and Avalanche Fuji-based smart contracts, storage via IPFS solutions, and AI for report validation, which offers increased levels of confidentiality, integrity, and chain of custody for such digital information once processed. Empirical performance evaluation illustrates low latency, low fees, and anti-tampering. Potential works for the future include multilingual reports, improved mobile UX, and adversarial AI mitigation.

References

1. Mahmoud, A., El-Sayed, H.: ReACT-OCRS: AI-Driven Anonymous Online Cyber-Crime Reporting System (2025).
2. Khiari, F., Woungang, I., Anpalagan, A.: Compliance and Transparency in Digital Forensics Using Blockchain (2025).
3. Elgohary, A., Bayoumi, M., Abdelrahman, O.: Improving Chain of Custody for Image Forensics Using Blockchain (2022).
4. Stoyanova, K., et al.: Blockchain-Based Digital Evidence Management for IoT Forensics (2020).
5. Sharma, R., Gupta, S.: Survey of Cybercrime and Investigation Techniques (2021).
6. Salleras, A., et al.: Blockchain for Securing Digital Evidence: A Review (2022).
7. Liu, Y., Zhang, L., Chen, J.: Blockchain Framework for Secure Digital Evidence Management (2020).
8. Khan, M., Parkinson, S., Qin, Y.: Digital Forensics and Blockchain Review (2022).
9. Hossain, M., Muhammad, G.: Explainable AI for Crime Reporting Systems (2021).
10. Shah, M., Albakri, S., Khan, M.: Blockchain-Based Citizen Crime Reporting Platforms (2021).