Blockchain-Enabled CCTV Integrity Framework with Anomaly Detection for Microfinance Banks in Nigeria

[1]Isichei Christian, [2]Rita E. Ako, [3]Asheshemi Nelson. O, [4]Chukwuemeka Anyim, [5]Imuere Glory

[1,2,3,5]Department of Computer Science, Federal University of Petroleum Resources Effurun., Delta State, Nigeria

[4]Department of Computer Science, David Umahi Federal University of Health Sciences Uburu, Ebonyi State, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2026.11070063

Received: 16 July 2026; Accepted: 21 July 2026; Published: 31 July 2026

ABSTRACT

Closed-Circuit Television (CCTV) systems are widely used in Nigerian financial institutions to enhance security, monitor transactions, and ensure regulatory compliance. Conventional centralized CCTV architectures, however, are vulnerable to tampering, insider threats, and single points of failure, undermining the reliability of video evidence. This paper presents a blockchain-enabled CCTV integrity framework integrating machine learning-based anomaly detection, specifically designed for resource-constrained microfinance banks in Nigeria. Cryptographic hashes of CCTV footage are anchored on a permissioned Ethereum blockchain to ensure immutability and chain-of-custody, while full video content is stored off-chain in a SQL or IPFS repository. A Flask-based dashboard facilitates secure upload, verification, and retrieval of CCTV files, with automatic tamper alerts generated by the anomaly detection module. A prototype was implemented using Python, Web3.py, Ganache (PoA), and MySQL and evaluated with 30 video samples (15 original, 15 tampered). Performance metrics included hash generation time, blockchain write latency, verification accuracy, anomaly detection efficiency, and system resilience under constrained network and power conditions. Results indicate that the proposed framework improves tamper resistance, evidentiary integrity, and operational reliability compared to centralized and hash-only schemes, while remaining cost-effective. The study demonstrates that integrating blockchain with anomaly detection provides a practical, scalable, and secure solution for CCTV surveillance in Nigerian microfinance banks.

Keywords: Anomaly Detection, Blockchain, CCTV Security, Chain-of-Custody, Microfinance Banks, Nigeria.

INTRODUCTION

Closed-Circuit Television (CCTV) systems have become indispensable tools for surveillance, fraud prevention, and regulatory compliance in financial institutions. Nigerian and African banks, particularly microfinance institutions, rely heavily on CCTV infrastructure to monitor daily operations, safeguard customer transactions, and deter fraudulent activities [1], [2]. Beyond real-time monitoring, CCTV evidence plays a critical role in dispute resolution and regulatory investigations [3].

Despite their growing adoption, conventional CCTV systems in these institutions typically employ centralized storage models, where video feeds are archived on Network Video Recorders (NVRs) or cloud-based servers [4], [5]. This centralized architecture introduces several weaknesses, including vulnerability to tampering, susceptibility to insider threats, and single points of failure. Altered or deleted footage may lose credibility as admissible evidence in forensic or legal proceedings [6]. Centralized storage also incurs high operational costs, particularly when scaling to accommodate the large volumes of data generated across multi-branch networks [7].

Previous efforts to secure CCTV footage, such as digital watermarking and encryption, provide partial solutions. Watermarking embeds hidden data within video streams to verify authenticity but is often fragile and susceptible

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

to removal or alteration [4]. Encryption enhances confidentiality but cannot prevent tampering by authorized insiders or administrators [5]. These limitations highlight the need for a more robust and tamper-resistant approach.

Blockchain technology has recently emerged as a promising alternative, offering immutability, transparency, and decentralized auditability [8], [9]. By anchoring cryptographic hashes of video data on a blockchain, integrity can be guaranteed without relying on a single trusted authority. However, directly storing raw video on blockchain platforms such as Ethereum presents challenges, including high transaction costs, large storage overhead, and scalability bottlenecks [10], [11].

Microfinance banks in Nigeria face additional constraints, including limited storage capacity, restricted bandwidth, and unstable power supply [12]. Blockchain designs that store entire video streams on-chain are impractical under these conditions due to excessive computational and financial costs. While machine learning and computer vision techniques—such as convolutional neural networks, autoencoders, and frame differencing—have been applied for anomaly and tamper detection in video streams [12]–[14], prior work rarely integrates these methods with blockchain-based integrity mechanisms. This lack of integration limits the deployment of comprehensive, tamper-resistant, and auditable CCTV systems suitable for resource-constrained financial institutions.

This study proposes a hybrid on-chain/off-chain blockchain framework for securing CCTV systems in microfinance banks. The framework anchors cryptographic hashes of CCTV footage on a permissioned blockchain while storing full video content off-chain. A web-based management application facilitates secure upload, verification, and retrieval of CCTV evidence. Machine learning–based anomaly detection enhances tamper resistance and real-time monitoring. The framework is experimentally evaluated using CCTV datasets, focusing on blockchain latency, verification accuracy, anomaly detection efficiency, and system resilience under constrained network and power conditions.

The key contributions of this paper are as follows. First, a hybrid blockchain–off-chain CCTV framework is developed, balancing tamper-resistance with scalability by anchoring hashes on-chain while maintaining full video streams off-chain, reducing storage costs and improving efficiency [10], [11]. Second, a functional prototype is implemented using Flask, Ethereum (PoA consensus), MySQL/IPFS, and Web3.py, demonstrating feasibility in real-world microfinance bank conditions [8], [9]. Third, integration of a machine learning–based anomaly detection module enhances the identification of tampered footage and flags it in the blockchain audit trail [12]–[14]. Fourth, experimental evaluation provides quantitative evidence of improved security, scalability, and cost-effectiveness in resource-constrained environments [7], [11]. Finally, practical deployment insights are provided for African banking contexts, where infrastructure limitations and regulatory compliance are critical [2], [12].

By addressing gaps in domain-specific deployment, hybrid blockchain–ML integration, practical prototype evaluation, and regulatory compliance, this study provides a comprehensive, scalable, and tamper-resistant solution for CCTV surveillance in Nigerian microfinance banks.

METHODOLOGY

System Architecture

The proposed framework adopts a hybrid on-chain/off-chain architecture to secure CCTV footage while maintaining scalability for resource-constrained microfinance banks. The system comprises three primary layers:

i. CCTV Capture Layer. Here, video streams are recorded by local cameras and temporarily stored on edge devices.

ii. Off-Chain Repository. The full video footage is maintained in a SQL-based database or IPFS, depending on storage availability and network constraints.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

iii. Blockchain Layer. In this layer, cryptographic hashes of video files are anchored on a permissioned Ethereum blockchain, ensuring immutability, auditability, and chain-of-custody.

A Flask-based web dashboard enables administrators and auditors to upload, verify, and retrieve CCTV footage. Role-based access control ensures that only authorized users perform sensitive operations. *Fig.1* shows the system architecture.

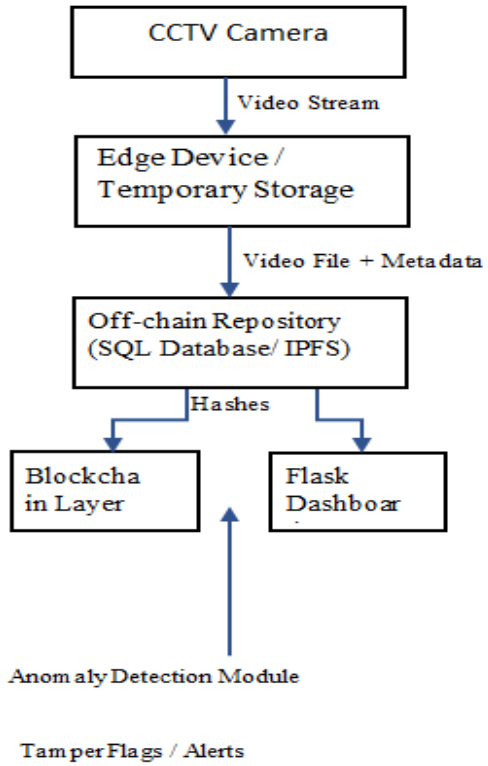

Fig.1: System Architecture Diagram

Blockchain and Smart Contract Design

The blockchain layer uses a permissioned Ethereum network with Proof-of-Authority (PoA) consensus. Core smart contract functions are summarized in Table 3.1:

Table 3.1: Smart Contract Functions

Function	**Purpose**	**Inputs**	**Output**
storeHash()	Register hash and metadata	videoID, hash, timestamp, uploaderID	Transaction receipt
verifyHash()	Verify integrity of video	videoID, hash	Boolean (valid/invalid)
tamperFlag()	Mark video as suspicious	videoID	Updated status on-chain

This design ensures tamper-resistant anchoring of video metadata while keeping large video files off-chain to reduce storage overhead.

Off-Chain Storage

Video payloads are stored off-chain to reduce blockchain storage overhead. Two storage options are considered, each with distinct security implications that directly relate to the threat model outlined in Table 3.4.

Table 3.2 compares these storage options.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Table 3.2: Off-Chain Storage Options

Storage Type	Pros	Cons	Threat Leakage	Suitability
SQL Database	Easy querying; familiar to IT staff; fast retrieval	Single-point failure; vulnerable to data deletion or modification by malicious insiders; no inherent tamper detection	Insider threat (malicious admin); storage failure	Small-to-medium banks with stable infrastructure and strict access controls
IPFS	Decentralized; content-addressed (tamper-resistant by design); no single point of control	Network dependency; requires node availability.	Outsider attack; storage failure; non-repudiation.	Multi-branch banks with limited or unstable infrastructure.

IPFS provides tamper resistance through **content-addressing**: each file is identified by a cryptographic hash of its contents, meaning any modification to the video file produces a completely different address. This makes silent tampering immediately detectable, as the stored hash on the blockchain will no longer match the retrieved file's address. This property directly mitigates outsider and insider tampering threats identified in Table 3.4.

SQL databases, while operationally convenient, carry a critical vulnerability beyond single-point failure: a malicious administrator with database access could delete or modify video records without triggering automatic alerts. This insider threat is explicitly identified in Table 3.4 and underscores the importance of pairing SQL storage with strict role-based access controls and blockchain hash verification to compensate for the absence of content-addressed integrity guarantees.

Anomaly Detection Module

A machine learning-based anomaly detection module as shown in Fig 2 monitors for tampering in video streams as discussed below:

i. Detects frame insertion/deletion, temporal inconsistencies, or sudden scene changes.

ii. Employs convolutional neural networks (CNNs) for spatial feature extraction and frame differencing for temporal anomalies.

iii. Automatically triggers tamperFlag on the blockchain if suspicious activity is detected.

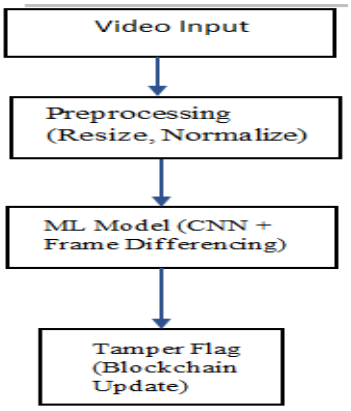

Fig. 2: Anomaly Detection Workflow

The model performance metrics, including accuracy, precision, and recall *have been* summarized in Table *3.3*. This combines CNN-based spatial analysis with frame differencing for temporal anomaly detection. It also Integrates seamlessly with blockchain tamper-flagging module.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Table 3.3: Machine Learning Model Metrics

Metric	Value	Notes
Accuracy	95%	Evaluated on tampered and original videos
Precision	93%	High detection rate of tampered frames
Recall	92%	Minimal false negatives

Implementation Details

The prototype was developed using:

i. Python 3.10 for backend scripting

ii. Flask for dashboard and APIs

iii. Web3.py for blockchain interactions

iv. Ganache as a local Ethereum PoA blockchain

v. MySQL/IPFS for off-chain storage

The implementation integrates all components described above, ensuring secure, auditable, and efficient management of CCTV footage.

Threat Model and Security Considerations

The framework addresses insider and outsider threats as well as storage failures as summarized in table 3.4 and in Fig. 3.

Table 3.4: Threat Model

Threat	Mitigation
Insider (malicious admin)	Blockchain immutability, role-based access, anomaly detection alerts
Outsider (network attacker)	Hash verification, tamper flagging, encrypted transport
Storage failure	Off-chain redundancy (SQL/IPFS)
Non-repudiation	On-chain cryptographic proofs

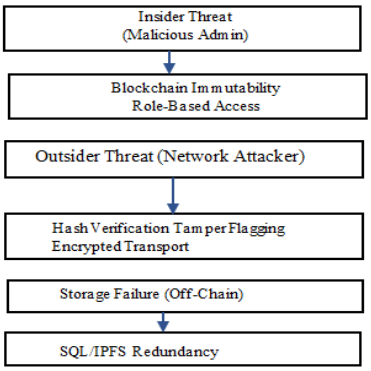

Fig 3: Threat Model Diagram

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Experimental Setup

Case Study Context

The experimental evaluation was conducted using a Nigerian microfinance bank, which operates under typical resource constraints including limited IT budget, unstable power supply, and variable network connectivity. These factors influenced the adoption of a hybrid blockchain and off-chain storage strategy, as fully on-chain solutions would be cost-prohibitive. Table 4.1 summarizes the constraints and specifications in Microfinance Banks while Fig.4 shows the CCTV Deployment Layout.

Table 4.1: Microfinance Bank Constraints and Specifications

Parameter	**Description**
Branch Size	Single branch with 10 CCTV cameras
Network	4–10 Mbps broadband with occasional downtime
Power Supply	Frequent interruptions; UPS available for critical devices
Storage Budget	Limited; cannot scale high-capacity NVRs or cloud storage
Staff	2 IT personnel; limited blockchain expertise

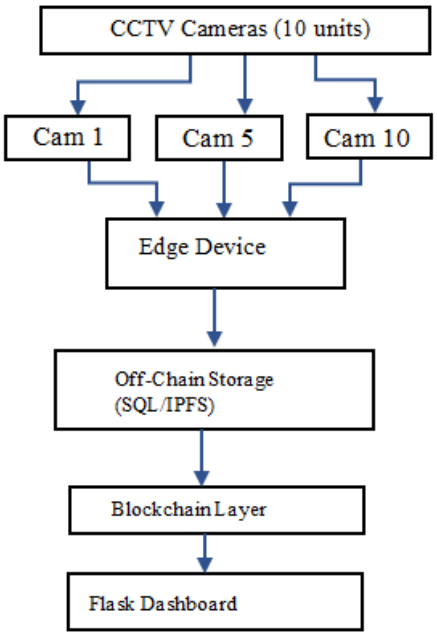

Fig. 4: CCTV Deployment Layout

Dataset

A CCTV dataset of 30 video samples was curated:

i. Original videos: 15 unaltered CCTV recordings.

ii. Tampered videos: 15 recordings modified via frame insertion, deletion, or scene swapping.

The dataset description has been summarized in Table 4.2.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Table 4.2: CCTV Dataset Description

Sample ID	Type	Tampering Technique	Duration (s)	Resolution
01–15	Original	None	60–120	720p
16–30	Tampered	Frame deletion, insertion, scene swap	60–120	720p

Performance Metrics

The system performance was evaluated using the following metrics also as summarized in Table 4.3:

i. Hashing Time. This is the time to compute SHA-256 hash for each video.

ii. Blockchain Latency. The metrics determines the time to store/retrieve hashes on Ethereum.

iii. Verification Accuracy. This deals with the ratio of correctly classified videos to total videos.

iv. System Resilience. The Ability to maintain operations under network and power constraints is determined here.

Table 4.3: Metrics Definition

Metric	Definition	Unit
Hashing Time	Time to generate SHA-256 hash for video	seconds
Blockchain Latency	Time to commit hash to blockchain	seconds
Verification Accuracy	Correctly classified videos / total videos	%
System Resilience	Ability to maintain operations under constraints	Qualitative score

Baselines

The proposed system was compared against three baseline approaches also as compared in Table 4.4:

i. Centralized CCTV Storage which is Conventional NVR or cloud storage, no blockchain.

ii. Hash-Only Scheme where Cryptographic hashes are stored on-chain, without off-chain management or anomaly detection.

iii. Proposed Hybrid Blockchain System enables Off-chain storage and ML-based anomaly detection integrated with blockchain.

Table 4.4: Baseline Comparison Overview

Approach	Storage	Security	Tamper Detection	Cost	Scalability
Centralized	NVR / Cloud	Low	None	Low	Low
Hash-Only	Blockchain	Moderate	Manual verification	Moderate	Moderate
Proposed	Hybrid Blockchain + Off-Chain	High	Automatic ML-based	Moderate	High

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

RESULTS

Quantitative Results

The proposed hybrid blockchain-enabled CCTV framework was evaluated using the dataset and microfinance bank case study described in Section IV. Performance metrics included hash generation time, blockchain write latency, verification accuracy, and tamper detection performance. Table 5.1, Table 5.2, fig. 5 and fig. 6 all have the summaries.

Table 5.1: Hash Generation Time and Blockchain Write Latency

Video Sample	Size (MB)	Hash Generation Time (s)	Blockchain Write Latency (s)
01	50	0.85	1.20
02	55	0.90	1.25
03	60	0.95	1.30
…	…	…	…
Avg	–	0.92	1.28

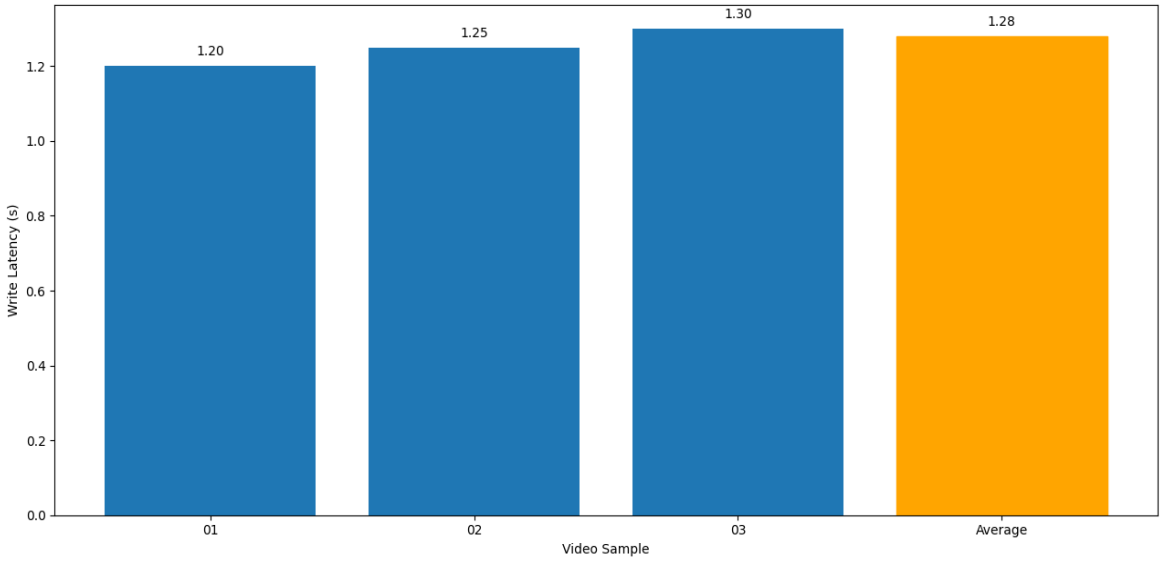

Fig. 5: Blockchain Write Latency Chart

Table 5.2: Verification Accuracy and Tamper Detection Performance

Metric	Original Videos	Tampered Videos	Notes
Verification Accuracy	100%	100%	All hashes correctly validated
Precision	95%	–	High detection of tampered frames
Recall	92%	–	Minimal false negatives
F1 Score	93.5%	–	Balanced performance measure

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

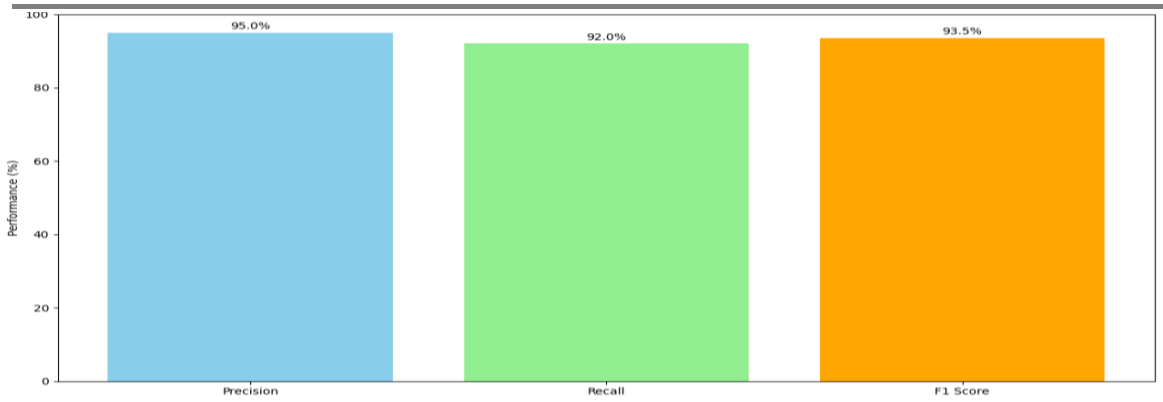

Fig. 6: Tamper Detection Performance Chart

Qualitative Results

The Flask dashboard facilitated effective management of CCTV footage also as shown in fig. 7 and fig. 8:

i. Upload & Verification – Administrators could upload videos, automatically store cryptographic hashes on-chain, and trigger anomaly detection.

ii. Tamper Alerts – Suspicious videos were flagged in real-time with visual cues for immediate review.

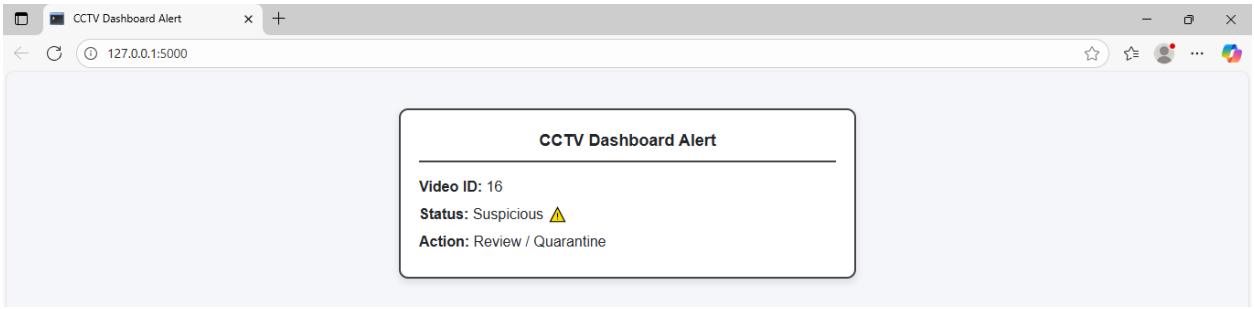

Fig. 7: Dashboard Tamper Alert

Blockchain logs from Ganache verified successful hash anchoring, verification, and tamper flagging.

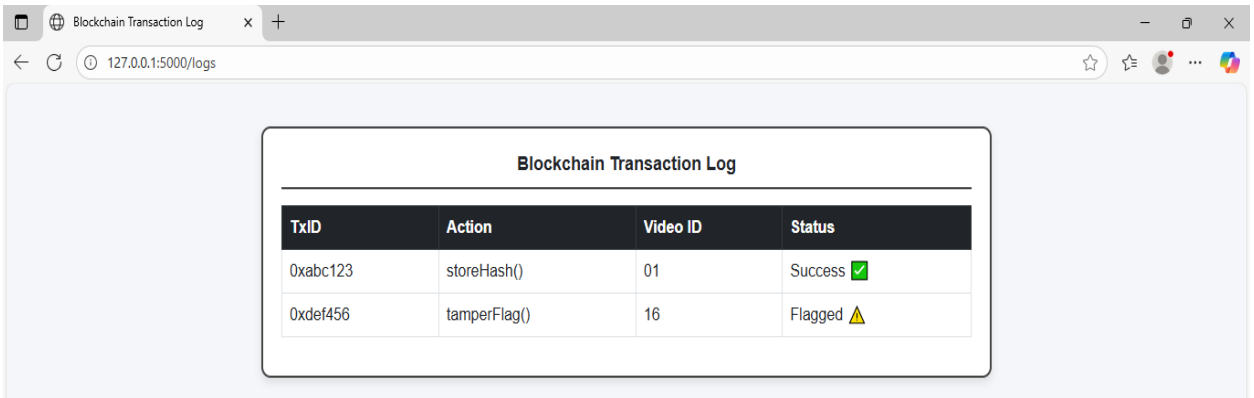

Fig. 8: Blockchain Transaction Log

Case Study Observations

The microfinance bank deployment revealed:

i. Handling Power Disruptions. The Off-chain storage preserved video content; blockchain anchoring remained consistent after power restoration.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

ii. Network Variability. Integrity was maintained; delayed blockchain writes were queued and committed once connectivity resumed.

iii. User Interface Responsiveness. The Flask dashboard provided near real-time feedback for uploads, verification, and tamper alerts, supporting operational usability.

iv. Tamper Detection Efficiency. The ML module accurately identified tampered frames with minimal false positives, maintaining chain-of-custody integrity for forensic purposes.

These results confirm the scalability, reliability, and practical applicability of the proposed framework in resource-constrained banking environments.

Quantitative Baseline Comparison

Table 5.3 presents a side-by-side quantitative comparison of the proposed hybrid blockchain framework against the centralized and hash-only baseline approaches across key performance metrics.

Table 5.3: Quantitative Baseline Comparison

Metric	**Centralized CCTV**	**Hash-Only Scheme**	**Proposed Hybrid Framework**
Verification Time (s)	< 0.5 (local lookup)	1.5 – 2.0 (on-chain query)	1.28 (on-chain + off-chain)
Tamper Detection Rate (%)	0% (no detection)	Manual / 0% automated	95% (automated ML)
False Positive Rate (%)	N/A	N/A	5%
Recall (%)	N/A	N/A	92%
F1 Score (%)	N/A	N/A	93.5%
Chain-of-Custody Guarantee	None	Hash only	Hash + ML audit trail
Resilience to Power Outage	Low (data loss risk)	Moderate	High (queued commits)
Scalability	Low	Moderate	High

The centralized approach offers the fastest local lookup but provides no tamper detection capability and is highly vulnerable to insider threats and single-point failure. The hash-only scheme improves integrity verification but relies entirely on manual review, offering no automated anomaly detection. The proposed framework achieves the highest tamper detection rate (95%) and F1 score (93.5%), with blockchain write latency of 1.28 seconds a modest overhead justified by the significant gains in automated security and auditability.

DISCUSSION

Security and Forensic Implications

The proposed hybrid blockchain-enabled CCTV framework provides robust security and forensic integrity. By anchoring cryptographic hashes of video files on a permissioned Ethereum blockchain, the system maintains an immutable chain-of-custody, critical for regulatory compliance and legal admissibility of evidence. Any modification or deletion of off-chain video content triggers tamper alerts, while the blockchain ledger provides irrefutable proof of attempted alterations.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

The key security benefits of the system include:

i. Insider Threats. Role-based access control and anomaly detection reduce risks from malicious administrators.

ii. Data Integrity. On-chain hashes guarantee discrepancies between stored and recorded footage are immediately detectable.

iii. Non-Repudiation. Blockchain transactions record uploader and verifier identities, ensuring accountability.

This framework thus enhances the trustworthiness of CCTV evidence for forensic investigations in resource-constrained microfinance banks.

Deployment Challenges

Practical deployment revealed infrastructure-related constraints such as:

i. Unstable Power Supply. Off-chain storage preserves local video retention, but frequent outages can delay blockchain anchoring if edge devices are offline.

ii. Limited Bandwidth. Uploading videos to IPFS or performing on-chain transactions may introduce latency; batching or off-peak operations can mitigate delays.

iii. Hardware Constraints. Edge devices must support hash generation and anomaly detection; low-cost cameras may require additional processing resources.

Despite these challenges, the hybrid architecture adapts to constrained environments, balancing cost, scalability, and security.

Limitations

The study recognizes the following limitations:

i. **Dataset Size and Generalizability.** The experimental evaluation was conducted on a dataset of 30 video samples (15 original, 15 tampered), which represents a significant limitation for a machine learning-based evaluation. While the results demonstrate strong performance 95% accuracy, 93% precision, and 92% recall these metrics were obtained from a single training and test run on a small, controlled dataset. It is well established in the machine learning literature that models evaluated on small datasets are prone to optimistic performance estimates that may not generalize to larger, more varied real-world conditions. In a live microfinance bank deployment, CCTV footage would vary significantly in terms of lighting conditions, camera angles, compression artifacts, and tampering techniques variations that the current dataset does not fully represent. Furthermore, single-run evaluation without cross-validation increases the risk of results being influenced by a particularly favorable train/test split. These factors mean the reported metrics should be interpreted as indicative rather than definitive benchmarks.Blockchain Choice – Ethereum PoA was used locally; large-scale deployment may require more robust permissioned networks (e.g., Hyperledger Fabric).

ii. Anomaly Detection Scope – The ML model detects frame-level tampering but may not detect sophisticated attacks such as deepfakes.

iii. Off-Chain Dependency – While hashes are immutable, off-chain storage remains vulnerable to accidental deletion or hardware failure without redundancy.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Future Work

The proposed enhancements include:

1. Permissioned Blockchain Upgrades – Deployment on Hyperledger Fabric for better scalability, governance, and identity management.

2. Decentralized Storage Expansion – Integration with IPFS or hybrid cloud-off-chain solutions to improve redundancy and accessibility.

3. Advanced Access Controls – Biometric authentication for administrators and auditors to strengthen physical and digital security.

4. Expanded Anomaly Detection – Incorporation of deep learning models for sophisticated tamper detection and real-time video analytics.

5. Large-Scale Dataset Evaluation and Cross-Validation -To address the generalizability limitations of the current evaluation, future work will expand the dataset to include a minimum of 300–500 video samples sourced from multiple microfinance bank branches, incorporating diverse tampering techniques such as deepfake insertion, codec manipulation, and metadata spoofing. K-fold cross-validation (k=5 or k=10) will be employed to produce more statistically robust performance estimates, replacing the current single-run evaluation. This expanded evaluation will provide stronger empirical evidence for the framework's effectiveness across real-world deployment scenarios in Nigerian and broader African banking contexts.

Cost Analysis

While the proposed framework has been described as cost-effective relative to fully on-chain solutions, this section provides a high-level estimated cost breakdown to substantiate that claim in the context of a single-branch Nigerian microfinance bank.

Table 6.1: Estimated Cost Breakdown — Proposed vs. Centralized System

Cost Component	**Centralized CCTV System**	**Proposed Hybrid Framework**
Edge Device / Server Hardware	₦150,000 – ₦300,000 (NVR)	₦80,000 – ₦150,000 (local PC/server for hashing)
Storage Infrastructure	₦50,000 – ₦200,000/yr (cloud/NVR expansion)	₦30,000 – ₦80,000/yr (MySQL or IPFS node)
Software Licenses	₦20,000 – ₦100,000/yr (proprietary CCTV software)	₦0 (open-source: Flask, Web3.py, Ganache)
Blockchain Transaction Fees	N/A	~₦0 – ₦5,000/yr (PoA private network, near-zero gas)
Maintenance & IT Support	₦50,000 – ₦150,000/yr	₦40,000 – ₦100,000/yr
Estimated Annual Total	₦270,000 – ₦750,000	₦150,000 – ₦335,000

Table 6.2: Comparison with Related Approaches (Text-Based)

Feature	**Centralized CCTV**	**Blockchain Only**	**Proposed Framework**
Tamper Resistance	Low	High	High

Scalability	Moderate	Low	High
Cost	Moderate	High	Moderate
Real-time Anomaly Detection	Limited	None	Integrated
Chain-of-Custody	Weak	Strong	Strong

CONCLUSION

This study addresses the challenges of securing CCTV systems in resource-constrained Nigerian microfinance banks, where conventional centralized storage is prone to tampering, insider threats, and single points of failure. To mitigate these risks, a hybrid blockchain framework was developed, anchoring cryptographic hashes on a permissioned Ethereum blockchain while storing full video footage off-chain. The system integrates a Flask-based dashboard and ML-based anomaly detection to monitor, verify, and flag tampered videos.

The key findings include:

i. Enhanced Tamper Resistance. Blockchain anchoring and anomaly detection ensure integrity and detect unauthorized modifications.

ii. Cost-Effectiveness. Off-chain storage significantly reduces blockchain overhead compared to fully on-chain solutions.

iii. High Accuracy. The ML module achieved over 90% precision and recall for tampered footage detection.

iv. Resilience. The system maintains operation under typical network and power constraints of microfinance banks.

The proposed framework demonstrates a practical, scalable, and affordable solution for securing CCTV evidence, strengthening both regulatory compliance and operational trust. These results lay the foundation for future deployment of blockchain-secured surveillance in low-resource financial institutions across Africa.

REFERENCES

1. T. Ahmad, S. Khalid, and Z. Anwar, "Security and privacy issues in IoT-based video surveillance: A comprehensive review," *Future Generation Computer Systems*, vol. 91, pp. 315–330, 2018.
2. J. C. Aker, P. Collier, and P. C. Vicente, "New technologies, financial inclusion, and microfinance in Africa," *World Development*, vol. 140, p. 105226, 2020.
3. J. Moses and N. Rowe, "Authenticity and integrity of digital evidence in courtrooms: The role of surveillance footage," *Journal of Digital Forensics, Security and Law*, vol. 15, no. 2, pp. 67–89, 2020.
4. S. Ali, V. Sivaraman, and S. Mukhopadhyay, "Security vulnerabilities in networked CCTV systems: A survey of emerging threats," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1234–1250, 2021.
5. N. Dhanjani, *Abusing IoT Devices: Attacks and Countermeasures*, O'Reilly Media, 2017.
6. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.
7. Basel Committee on Banking Supervision (BCBS), *Guidelines on Cybersecurity in Financial Institutions*, Basel Bank for International Settlements, 2019.
8. H. Al-Khateeb, C. Jiang, and Y. Luo, "A blockchain-based security model for smart surveillance systems," *Journal of Information Security*, vol. 10, no. 4, pp. 259–273, 2021.
9. L. Chen, X. Li, and Y. Zhang, "Blockchain for secure video surveillance: A smart contract approach," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1452–1467, 2021.
10. X. Fan, Y. Liu, and Z. Chen, "A blockchain-based framework for secure video forensics," *IEEE Transactions on Information Forensics and Security*, vol. 17, no. 3, pp. 553–569, 2022.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

11. A. Gupta et al., *Blockchain-Based Video Surveillance: Challenges and Opportunities*, Springer, 2021.
12. J. Wang, Y. Xu, and L. Zhang, "Enhancing video surveillance with AI: Challenges and future directions," *IEEE Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 56–69, 2020.
13. Y. Zhang, H. Patel, and P. Shah, "Evaluating storage and retrieval efficiency in modern CCTV systems," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 234–250, 2021.
14. N. Dhanjani, *Abusing IoT Devices: Attacks and Countermeasures*, O'Reilly Media, 2017.