[1]Mr. Himanshu Trale,

[2]Dr. Balaso Jagdale

Blockchain-Infused Log Resilience for Forensic Auditing

Journal of Electrical Systems

Abstract: - Digital forensics functions optimally due to the combined factors of intact log data and their easy accessibility. The conventional logging systems create major reliability concerns because they remain susceptible to altering, deleting and modifying information. The research evaluates how blockchain technology enhances log management systems by creating tamper-evident verifiable and resilient log record systems. This paper develops a blockchain-based architecture to enhance log trustworthiness and durability with an assessment of practical implementation aspects as well as illustrations of benefits and constraints during forensic auditing scenarios. The blockchain network functions as an autonomous system based on cryptography to generate time-stamped and autonomous log verifications beyond traditional authoritative control. The logs remain available to investigators during investigations because of this system even if internal systems experience breaches. This paper presents practical deployment guidance along with challenge descriptions as well as future research proposals which aim to maximize the blockchain-forensic logging integration.

Keywords: Blockchain Technology, Digital Forensics, Log Integrity, Tamper-Evident Logging, Forensic Auditing, Cryptographic Verification, Resilient Log Management.

Introduction

The foundation of forensic auditing in cybersecurity depends on digital logs for compliance and legal investigations and in cybersecurity. These electronic records document essential system activities together with user actions and transactions as well as significant events which will help establish incident reconstruction and accountability proof. But their value hinges on integrity. Any modification to a log or its deletion completely eliminates its credibility for court evidence. The centralized log storage method in databases makes them vulnerable to insider attacks and gets compromised by unauthorized access and advanced cyber threats.

Blockchain technology stands out because it maintains distributed database features with unchangeable data records. The integration of blockchain technology with logging instruments allows the establishment of an advanced system which permanently logs operations while adding cryptographic safeguards with timestamped documentation. This writing explores the integration of blockchain technology with logging systems to develop forensic resilience together with prevention against tampering and support for trustworthy auditing.

The continuous rise in complex cyber events creates substantial pressure for organizations to guarantee the intact state of their digital evidence. Online logging systems prove inadequate when used in hostile environmental settings to counter both internal threats and advanced persistent attacks.(Tian, H., Wang, J., Chang, C.-C., & Quan, H. (2020). A blockchain-based method establishes a fundamental change by making resilient distributed ledger components out of log records while lowering dependency on internal controls and creating advanced transparency measures. Growing importance of digital investigations within regulations and legal and operational domains makes blockchain-enhanced logging more necessary.

Aim and Objectives

Aim:

A team should develop a blockchain-embedded logging solution for digital forensics that delivers improved resistance alongside strengthened security and auditable characteristics to digital log files.

Objectives:

1. Review and understand the weaknesses that affect current forensic auditing log management systems.
2. A blockchain-based secure log design system requires development.
3. A simulation of a blockchain platform for logging will receive implementation.
4. Test the system for tamper detection along with data accessibility features.

Himanshu.tarale@mitwpu.edu.in [1]
Student (M.Tech) School of Computer Engineering & Technology[1]
Associate Professor School of Computer Engineering & Technology[2]
Dr. Vishwanath Karad MIT World Peace University INDIA

5. Examine the practical issues which will arise during actual implementation.

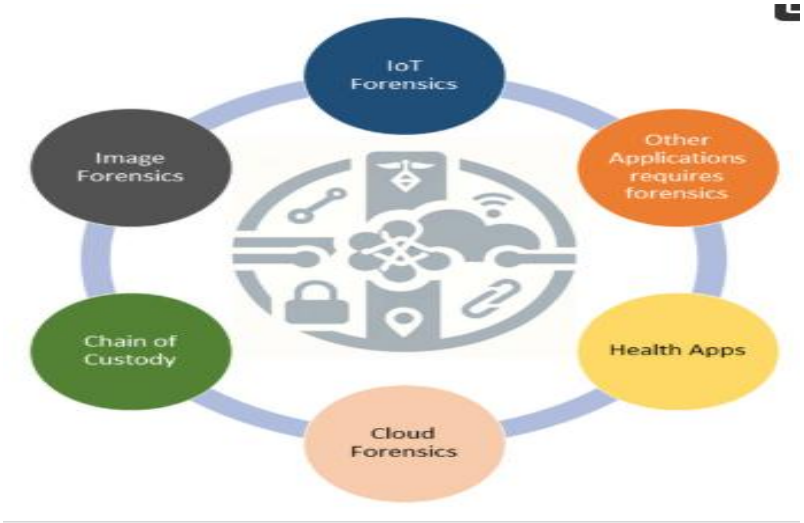

Figure 1 - The Proposed generic framework that can encapsulate all types of forensics transactions in blockchain.

Hypothesis

Implementing blockchain within log management systems creates logging systems that maintain unalterable records while being fully auditable and tamper-proof which results in superior forensic audit reliability.

Research Gap

A considerable number of studies explore robust logging systems and blockchain finance applications as well as supply chain blockchain solutions but this research area lacks sufficient examination of blockchain in forensic auditing. The current log management solutions operate without decentralized trust features while they remain at high risk for both insider attacks and advanced cyber intrusions. Existing blockchain security applications remain primarily theoretical because they lack proper frameworks which would match the specific needs of forensic investigations. This paper fills the existing gap by implementing a specific forensic log resilience analysis and practical architecture framework.

Literature Review

The article by Kshetri (2017) shows how blockchain establishes decentralized trust protocols to boost cybersecurity protection. Data privacy gets examined through blockchain according to Zyskind et al. (2015) because it shows great promise for safeguarding personal records from unauthorized access. Secures methods of logging have been developed by Lee and Kim (2019) through blockchain to establish forensic integrity. Although blockchain holds promise for boosting digital security according to this collective body of works it does not extensively explore forensic-oriented logging systems.(Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., & Mansell, J. (2021).

Most current logging systems maintain their data in centralized locations which creates.one vulnerable entry point. The distributed ledger architecture enables log metadata recording with full evidence of tampering prevention and absolute data persistence. Decentralized consensus and cryptographic hashing make blockchain able to validate log entry authenticity without disclosing what content exists within entries. Most recent studies in forensic auditing botch to deliver concrete implementation programs and operating models in the field which this research seeks to rectify.(Shakir, S., & None Ghulam Abbas. (2020).

Problem Statement

Log management systems currently do not include built-in features for digital integrity. Storage on local disks combined with server-based systems makes logs susceptible to the following threats.(Alqahtany, S. S., & Syed, T. A. (2024).

- Deleted by administrators or attackers.
- Altered to hide malicious activities.
- Rolled back using backups.
- The limitations of storage capacity force logs to overwrite each other because of existing rotation policies.

Digital forensics loses credibility because of this weakness in security systems. The absence of verified log scans leads investigators to encounter missing information as well as misleading reports and unattainable evidence. Access-controlled logging systems with backup systems still cannot block exploitation attempts made by privileged account holders and advanced cyber attackers.

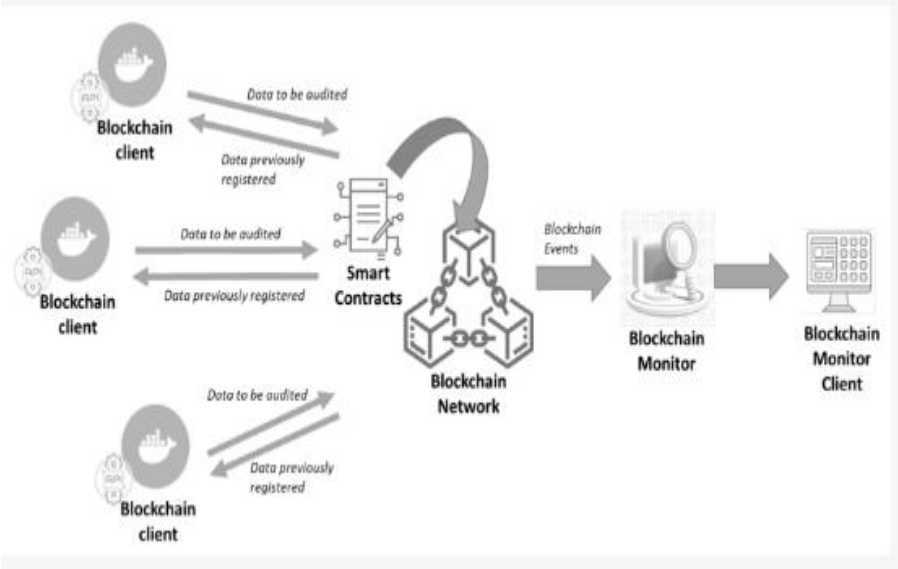

Figure 2 - Audit trail mechanism architecture.

Constructing an effective log framework presents the primary difficulty because organizations must achieve three essential objectives:

- Prevents or detects tampering.
- Preserves the chronological order of logs.
- Ensures long-term availability and auditability.(Gunjal, R. (2021).

Blockchain creates an encouraging base of operations for these requirements.

Methodology

The research adopted both design and evaluation as its research methodology. The initial step required reviewing literature on existing log management systems and their recognized flaws. Our evaluation of system weaknesses guided us to develop a new logging architecture which implements blockchain security features. The implementation of the new logging architecture used Hyperledger Fabric as the permissioned blockchain to conduct performance-based tests as well as tamper-detection assessments. User activities went into the system logs while the simulation used a process to confirm the integrity of these logs through time. Our evaluation process included active modifications of system logs followed by system detection of these altered logs. The last step involved analyzing system scalability as well as feasibility through performance testing under various workload scenarios.

Blockchain Fundamentals for Log Security

A distributed ledger system known as blockchain displays data across multiple network nodes using connected blocks where each new block includes cryptographic authentication from its preceding entry. Forensic logging benefits from the core features which include:

- After data insertion becomes part of the system it becomes impossible to change it in the past due to computational barriers.
- Each participant holds the ability to check all recorded entries into the system.
- Decentralization: No single point of control or failure.
- Each block contains cryptographic timestamps for protecting the sequential order.

Logs incorporated into blockchain functionality create entries which become permanent members of an authentic sequence of blocks. An attack on a system will leave blockchain-registered logs undamaged with their original contents.

Proposed Architecture: Blockchain-Infused Log Resilience System (BILRS)

BILRS functions as an integrated modular solution for existing logging frameworks based on the incorporation of blockchain features.

Components:

- The Log Collector utility receives all application and system log data as well as device records.
- Log Formatter & Hasher serves two functions: it convert raw logs into structured entries then calculates their hash value.
- The Blockchain Adapter function takes log hashes alongside timestamps and converts them into format that blockchain transactions can process.
- The blockchain layer operates as either a private blockchain network or a public one where log hashes get stored.
- The storage of authentic log content takes place in protected and encrypted storage facilities.(Guo, X., Li, D. A., & Zuo, Y. (2025).
- The Verifier Module functions to conduct cross-analysis between log entries and blockchain records for tampering detection.

Workflow:

- Logs are captured in real-time.
- Each log entry is hashed.
- The written information undergoes hashing procedures before it gets included into blockchain batches.
- Off-chain storage maintains entire log data through integrity connections to blockchain hash values.
- Auditors together with investigators conduct blockchain entry verification through the process of hash calculation followed by hash value comparison to blockchain records.

Implementation Considerations

Blockchain Type:

- The Ethereum blockchain and similar protocols keep logs highly intact while facing delays and expense challenges.
- The enabled blockchain network known as Hyperledger Fabric operates with enhanced speed together with enterprise-level authorization features.

Log Granularity:

The process of securing individual log entries adds protection but also raises expenses along with storage requirements. Merkle trees enable the hash computation process for log data which is grouped into batches (minute/hour durations).

Data Privacy:

Blockchain systems store only cryptographic hashes while omitting recorded data from its databases. Blockchains protect off-chain sensitive information through encryption which also works to decrease blockchain data storage needs.

Scalability:

Blockchain systems require high-frequency logging by adopting layer-2 solutions such as sidechains and rollups or by obtaining the ability to handle high transaction volumes.

Benefits of Blockchain-Based Log Resilience

Tamper Evidence:

Hash mismatch occurs following any modification to logs making it possible for automatic detection of alterations.(Liu, M., Wu, K., & Xu, J. (2019)

Audit Trail Integrity:

An unchanging sequence of logs appearing in chronological order proves advantageous for verifying chain-of-custody records.

Insider Threat Mitigation:

pıвileged users cannot change previously recorded logs. Operations they perform will always be detectable.

Long-Term Preservation:

Blockchain acts as a permanent proof ledger which remains intact regardless of the decommissioning of original systems.

Enhanced Legal Standing:

The permanent storage of data as logs serves as legitimate proof during compliance or judicial cases.

Challenges and Limitations

Storage and Cost Overhead: On-chain operations incur computational and sometimes financial costs. To achieve efficient system performance along with selective logging operations one must use the methods of efficient batching and selective logging.

Integration Complexity: The integration of blockchain interfaces with legacy systems requires either middleware solutions or customized connectors because legacy systems generally do not support those interfaces.

Trust Assumptions: Integrity within permissioned blockchains relies on proper governance of their nodes. Security can be impaired by administrator collusion with one another.

Real-Time Constraints: Without optimization the duration needed for creating blockchain records remains above real-time auditing requirements.

Case Study: Insider Breach Detection

A monitored system which tracks patient record access logs operates in this scenario. An administrator carrying out malicious activity tries to conceal unauthorized data access by removing log records from the system.

With BILRS in place:

- The blockchain incorporated hashed logs as new entries once the respective logs were completed seconds after creation.
- Auditors detect missing hashes during their standard verification process when deletion takes place.
- The blockchain records show the existence of particular logs making it clear that state tampering took place.
- The use of investigation occurs while investigators obtain legal backing through reinforced confidence.

Future Directions

- The system executes smart contracts to generate automated notifications at the instant it detects doubtful transaction events and mismatches in hash signatures.
- AI Integration: Analyze immutable logs for anomaly detection.
- Interoperability Standards: Develop common schemas for blockchain-based log exchange.
- Zero-Knowledge Proofs allow verifications of logs while keeping the contained information completely confidential.
- The log access system and digital signatures should operate through decentralized Identity schemes which verify user identities.

Conclusion

Forensic auditing demands absolute trust in digital logs. The current logging infrastructure systems cannot guarantee security against modern cyberthreats. The core of log management receives immutability and verifiable features through the blockchain operational paradigm. This document shows a blockchain-integrated architecture that advances log integrity and strengthens their resistance to attacks along with better forensic abilities. The system achieves tamper-evidence and supports extended auditability through robust log hashings combined with timestamping performed on distributed ledgers. We resolved operational problems regarding scalability and integration and privacy protection alongside the presentation of practical deployment solutions. The future research will concentrate on improving real-time functionality as well as standardizing interfaces together with legal framework evaluation. Blockchain integration into logging systems creates a significant technological progress for digital investigations by ensuring secure investigations in today's progressively digital environment.

References

[1] Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. Information, 15(2), 109. https://doi.org/10.3390/info15020109

[2] Gunjal, R. (2021). An Overview to Blockchain and Future of Accounting & Auditing in Blockchain Environment. The Management Accountant Journal, 56(11), 31. https://doi.org/10.33516/maj.v56i11.31-34p

[3] Guo, X., Li, D. A., & Zuo, Y. (2025). When Auditing Meets Blockchain: A Study on Applying Blockchain Smart Contracts in Auditing . SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5029553

[4] Guo, X., Zuo, Y., & Li, D. (2025). When auditing Meets Blockchain: A study on applying blockchain smart contracts in auditing. International Journal of Accounting Information Systems, 56, 100730. https://doi.org/10.1016/j.accinf.2025.100730

[5] Liu, M., Wu, K., & Xu, J. (2019). How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain. Current Issues in Auditing, 13(2). https://doi.org/10.2308/ciia-52540

[6] Md. Ezazul Islam, Md. Rafiqul Islam, Chetty, M., Lim, S., & Mehmood Chadhar. (2023). User authentication and access control to blockchain-based forensic log data. EURASIP Journal on Information Security, 2023(1). https://doi.org/10.1186/s13635-023-00142-3

[7] Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., & Mansell, J. (2021). A Blockchain-Based Audit Trail Mechanism: Design and Implementation. Algorithms, 14(12), 341. https://doi.org/10.3390/a14120341

[8] Shakir, S., & None Ghulam Abbas. (2020). Role of Forensic Auditing in Enhancing the Efficiency of Public Sector Organization. Reviews of Management Sciences, 2(2), 40–59. https://doi.org/10.53909/rms.02.02.030

[9] Sheng-Feng Hsieh, S.-F. H. (2021). Introduction to Blockchain in Accounting and Auditing. International Journal of Computer Auditing, 3(1), 037–039. https://doi.org/10.53106/256299802021120301006

[10] Tian, H., Wang, J., Chang, C.-C., & Quan, H. (2020). Public auditing of log integrity for shared cloud storage systems via blockchain. Wireless Networks. https://doi.org/10.1007/s11276-020-02373-5