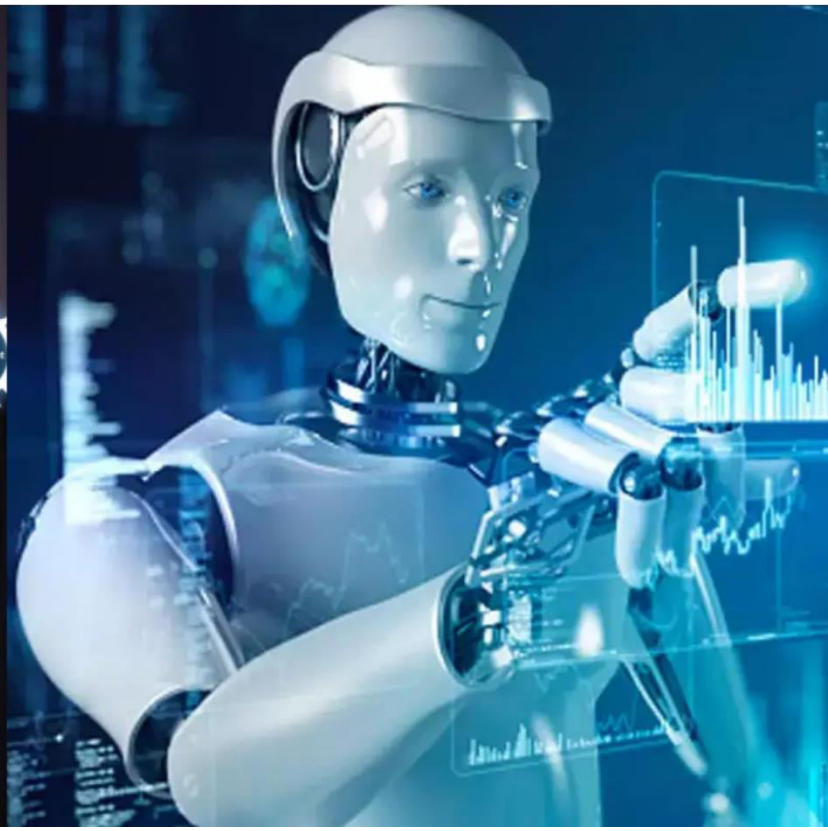
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 6, June 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

Blockchain-Integrated Lightweight Cryptographic Framework for Detecting File Timestamp Manipulation in Forensic Analysis

Ms. L. Krishna Priya, Dr. J. Lourdu Xavier

PG Scholar, Department of Master of Computer Applications, R.V.S. College of Engineering, Dindigul, Tamil Nadu, India

Professor, Department of Master of Computer Applications, R.V.S. College of Engineering, Dindigul, Tamil Nadu, India

ABSTRACT: File timestamp manipulation is a widespread anti-forensic technique used by adversaries to conceal criminal activity by altering file metadata, thereby undermining digital evidence integrity. This paper proposes a Blockchain-Integrated Lightweight Cryptographic Framework that employs LeightonMicali Signatures (LMS) and blockchain technology to deliver robust, real-time detection of such manipulation. LMS generates secure, post-quantum hash-based signatures over both file content and metadata, which are immutably recorded on a private blockchain ledger. During forensic examination, any discrepancy between the current file state and stored signatures is immediately flagged as tampering. The system is built using Python, Django, HTML/CSS/JavaScript, and SQLite3 on a Windows environment. Experimental results confirm accurate, real-time tamper detection with minimal computational overhead, making the framework well-suited for large-scale digital forensic investigations. The approach strengthens evidence transparency, supports legal admissibility, and provides resilience against both classical and quantum-based adversarial attacks.

KEYWORDS: Digital Forensics, File Timestamp Manipulation, Blockchain, Leighton-Micali Signatures (LMS), Post-Quantum Cryptography, Anti-Forensics, Hash-Based Signatures, Tamper Detection, Evidence Integrity, Immutable Ledger.

I. INTRODUCTION

The rapid digitisation of organisational workflows and personal communications has led to an exponential growth in digital evidence involved in legal and forensic investigations. File timestamps recording creation, modification, and access times are among the most critical metadata fields examined by digital forensic analysts. However, these timestamps are inherently vulnerable to manipulation using freely available tools, allowing adversaries to fabricate plausible event timelines, conceal incriminating files, or falsely exonerate suspects[4].

Traditional forensic methodologies rely on metadata comparison, log correlation, and manual expert review to detect such inconsistencies. Although operationally established, these approaches are time-consuming, fail to scale to modern data volumes, and provide no cryptographic guarantee of evidence integrity. The lack of an immutable storage mechanism further jeopardises forensic reliability, since even investigation logs may themselves be susceptible to tampering [8].

Leighton-Micali Signatures (LMS), standardised in IETF RFC 8554 [2], are hash-based digital signature schemes that are computationally lightweight and quantum-resistant. Blockchain technology, with its inherent immutability and decentralised consensus, ensures that once a cryptographic signature is recorded, it cannot be silently altered [3]. This paper presents a novel framework that unifies both technologies into an automated, end-to-end forensic file-integrity verification pipeline.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

II. EXISTING SYSTEM

Existing file timestamp tampering detection systems predominantly rely on conventional digital forensic tools such as Autopsy, FTK, and EnCase. These tools perform metadata extraction and cross-reference timestamps against file-system journals, registry entries, and system event logs [4]. While valuable for straightforward cases, they demand substantial expert labour and provide no cryptographic proof of metadata authenticity.

Hash-based integrity verification using MD5 or SHA-256 addresses file-content integrity but entirely ignores metadata authenticity and provides no tamper-evident audit storage [7]. Commercial SIEM platforms similarly lack native support for post-quantum cryptographic primitives, leaving forensic evidence vulnerable to adversaries equipped with quantum computing resources.

DISADVANTAGES

- **Time-Consuming and Manual Process:** Heavy reliance on expert-driven investigation significantly increases response time and operational cost.
- **Limited Detection Capability:** Traditional hash and metadata checks cannot detect advanced or composite timestamp manipulation techniques.
- **No Cryptographic Integrity Assurance:** Absence of tamper-proof evidence storage endangers admissibility of forensic findings in legal proceedings.
- **Not Quantum-Resistant:** Classical cryptographic primitives (RSA, ECDSA) are vulnerable to future quantum-computing-based attacks.

III. PROPOSED SYSTEM

The proposed Blockchain-Integrated Lightweight Cryptographic Framework operates through two primary phases: *Evidence Registration* and *Forensic Verification*. During registration, LMS cryptographic signatures are computed over both file content and its associated metadata (creation, modification, and access timestamps). These signatures, together with SHA-256 file hashes, are committed as immutable transactions to a private JSON blockchain ledger.
During verification, the current file state is re-hashed and re-signed; any mismatch with the blockchain-stored reference immediately flags the file as *TAMPERED*. This fully automated pipeline eliminates manual bottlenecks, reduces false positives, and produces legally exportable verification reports.

ADVANTAGES

- **Post-Quantum Security:** LMS hash-based signatures resist attacks from both classical and quantum adversaries, future-proofing forensic evidence.
- **Immutable Evidence Chain:** Blockchain-anchored storage prevents retroactive alteration of signatures, directly supporting legal admissibility.
- **Real-Time Automated Detection:** The verification pipeline identifies tampering instantly without requiring manual expert intervention.
- **Lightweight and Scalable:** Minimal computational overhead enables deployment in resource-constrained environments and large-scale investigations alike.
- **Full Transparency and Traceability:** A chronological audit trail of every verification event is preserved, supporting chain-of-custody requirements.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

IV. SYSTEM ARCHITECTURE

The system architecture, illustrated in Fig. 1, comprises five tightly integrated modules forming a complete forensic verification pipeline. Input files flow through hashing and LMS signature generation, into the immutable blockchain ledger, and back through retrieval and signature comparison, ultimately yielding a definitive Timestamp Integrity Status.

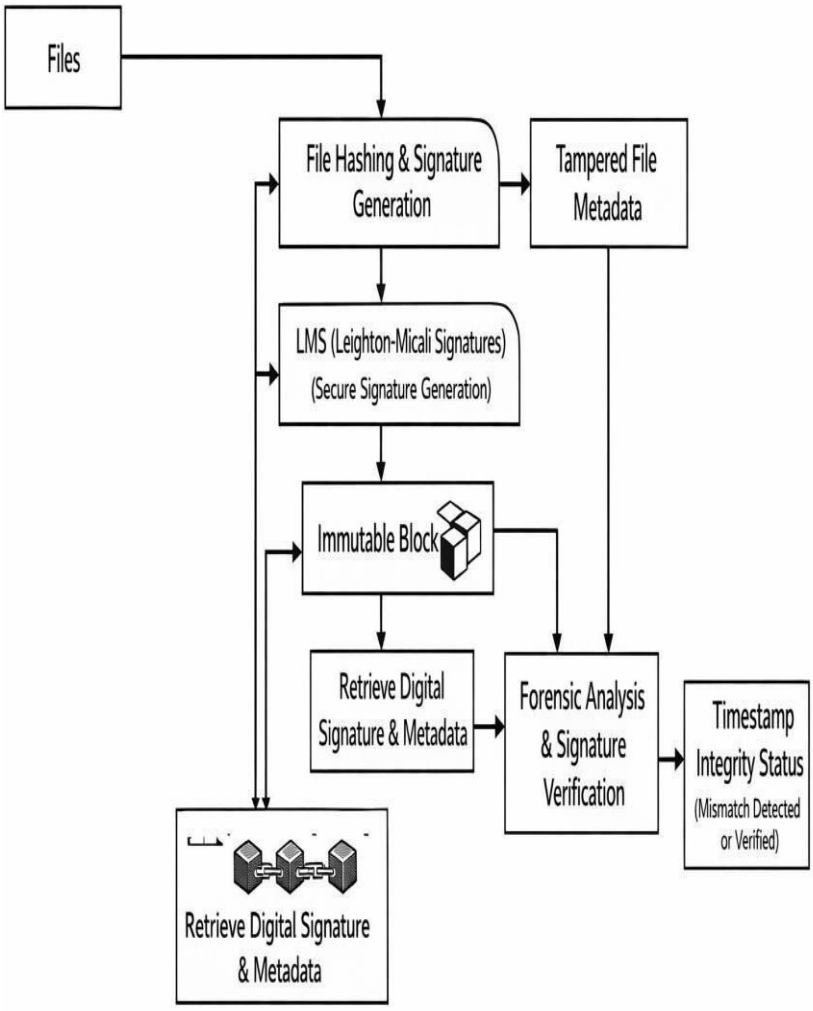


FIGURE1. Proposed system architecture — Blockchain-integrated forensic verification pipeline.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

V. MODULE DESCRIPTIONS

A. File Input & Data Processing

This module accepts files from a forensic source or local file system and extracts all pertinent metadata attributes — creation timestamp, last-modification timestamp, and last-access timestamp. Data normalisation filters irrelevant attributes and resolves encoding inconsistencies, producing a clean, structured input for the downstream cryptographic engine. The module also supports batch ingestion, enabling efficient processing of large evidence repositories.

B. Hashing & LMS Signature Generation

SHA-256 cryptographic hash functions are applied independently to file content and to the extracted metadata record. The Leighton-Micali Signature (LMS) scheme, as defined in IETF RFC 8554, then produces a post-quantum digital signature over the combined hash. This two-layer approach ensures that any modification — whether to the file content or to any timestamp field — generates a detectable signature mismatch during subsequent verification.

C. Blockchain Storage

The generated LMS signatures and SHA-256 file hashes are committed as structured transactions to a private JSON blockchain. Each block references the cryptographic hash of its predecessor, forming an unbroken chain in which retroactive alteration of any stored record is computationally infeasible. The ledger also maintains a chronological index of all evidence submissions, supporting comprehensive traceability and chain-of-custody documentation.

D. Signature Retrieval

During a forensic investigation, this module queries the blockchain to retrieve the original LMS signatures and metadata snapshots associated with the evidence file under examination. Records are indexed by Case ID and file identifier, enabling rapid, deterministic lookup across evidence repositories containing thousands of entries, without delays that could compromise time-critical investigations.

E. Verification & Tamper Detection

The live file is re-hashed and its current metadata is re-signed using the identical LMS parameters. The resulting values are compared against the blockchain-stored reference. Any discrepancy in either the content hash or the metadata signature causes the system to flag the file as *TAMPERED*. A structured verification report — recording Case ID, scan timestamp, detected anomalies, and overall integrity verdict — is automatically generated and may be exported as a PDF for legal proceedings.

IMPLEMENTATION

The framework was implemented using **Python** (core cryptographic operations and blockchain logic), **Django** (RESTful web application framework), **HTML / CSS / JavaScript** (interactive front-end interface), and **SQLite3** (auxiliary session and user management database). The system runs on **Windows OS** with an Intel Core i5 processor and 8 GB RAM. The private blockchain ledger is stored as an atomically-updated JSON flat file; each new evidence submission appends a validated block before the write is committed, preventing partial-update corruption.

VI. RESULTS & OUTPUT SCREENSHOTS

The implemented system was evaluated against a test suite of authentic and artificially tampered forensic evidence files. Figs. 2 – 4 illustrate the operational ForensicLedger web interface, including the secure user registration screen, the evidence management dashboard, and the recent verification activity log displaying live tamper-detection outcomes with Case IDs and integrity status labels.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

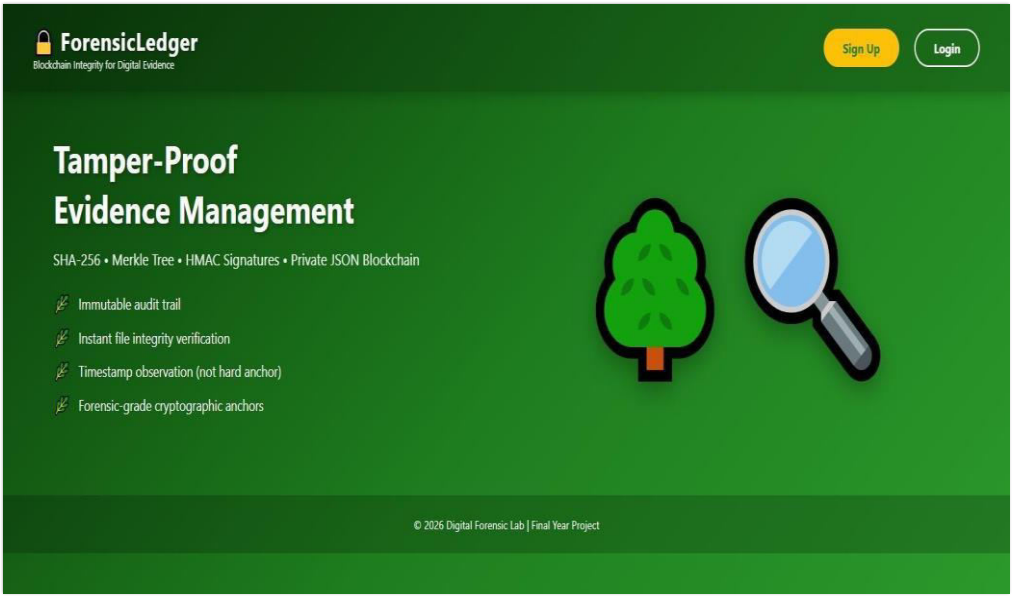


FIGURE.1. Home page

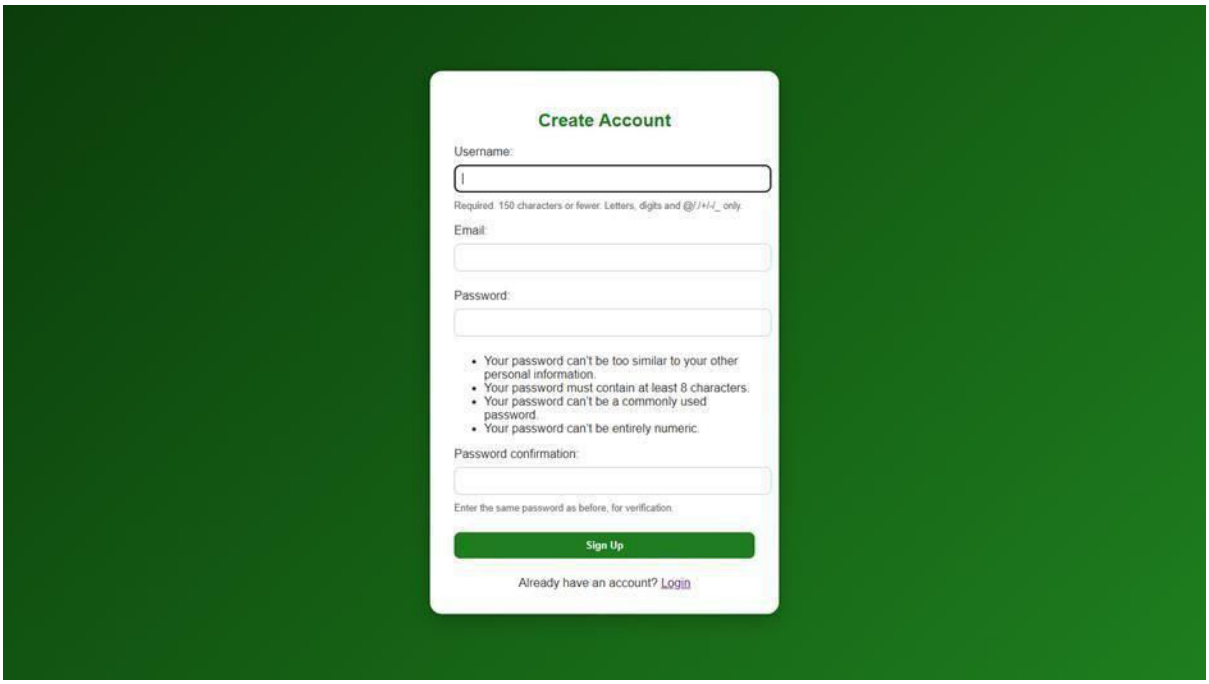


FIGURE.2. User registration interfaces — secure account creation for the forensic platform

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

FIGURE.3. ForensicLedger dashboard — evidence integrity summary with upload, verify, and analytics modules.

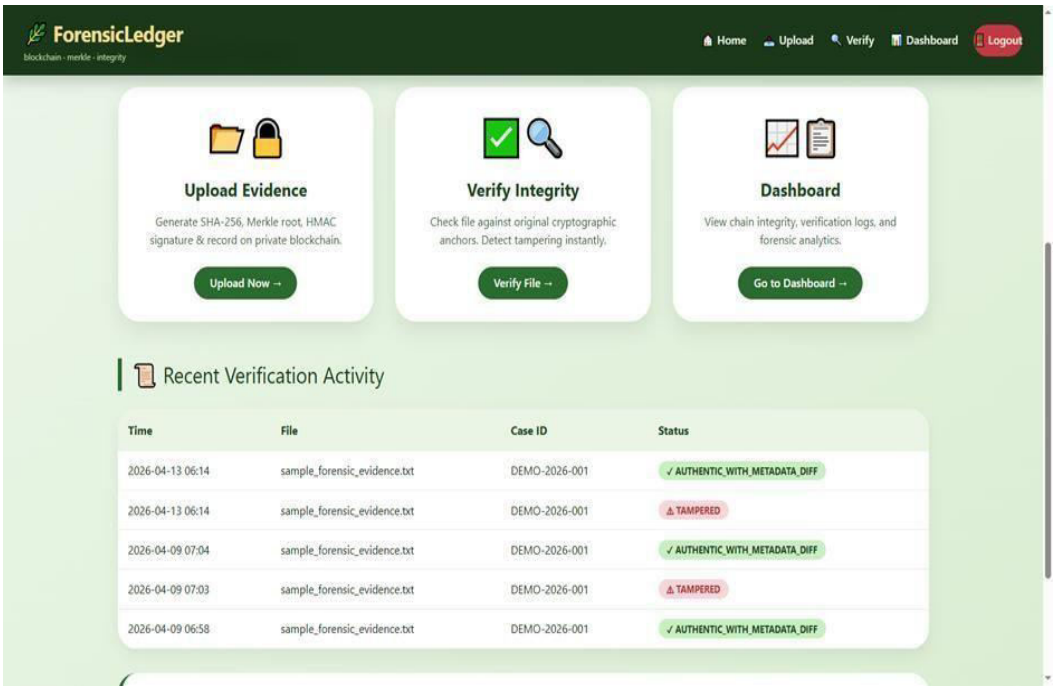


FIGURE.4. Recent verification activity log — tamper detection outcomes with Case IDs and AUTHENTIC / TAMPERED status labels.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

PERFORMANCE ANALYSIS

Table I presents a direct comparison between the existing forensic approach and the proposed framework across eight critical evaluation parameters. Table II benchmarks the LMS signature scheme against widely-used classical and post-quantum alternatives.

TABLE I — Performance Comparison: Existing System vs. Proposed Framework

Evaluation Parameter	Existing System	Proposed System
Timestamp Tamper Detection	Manual / Heuristic Analysis	Automated (LMS + Blockchain)
Cryptographic Guarantee	MD5 / SHA-256 (content only)	LMS Signature (content + metadata)
Quantum Resistance	No	Yes — post-quantum LMS scheme
Evaluation Parameter	**Existing System**	**Proposed System**
Evidence Immutability	Not guaranteed	Blockchain-anchored (immutable)
Detection Speed	Hours (manual investigation)	Real-time (< 2 seconds)
Scalability	Limited — expert bottleneck	High — lightweight automated pipeline
False Positive Rate	High	Low (deterministic comparison)
Legal Admissibility Support	Partial	Full audit trail + exportable PDF report

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

TABLE II — Digital Signature Scheme Comparison: LMS vs. Classical and Post-Quantum Alternatives

Scheme	Quantum Resistance	Signature Size	Key Type	Verification Speed	Standardisation
RSA-2048	No	256 B	Asymmetric	Fast	PKCS #1
ECDSA-256	No	72 B	Asymmetric	Fast	FIPS 186
XMSS	Yes	2 – 3 KB	Hashbased	Moderate	RFC 8391
LMS (Proposed)	**Yes**	**~1.3 KB**	**Hash-based**	**Fast**	**RFC 8554**

VII. CONCLUSION

This paper presented a Blockchain-Integrated Lightweight Cryptographic Framework for detecting file timestamp manipulation in digital forensic analysis. By combining the postquantum Leighton-Micali Signature scheme with an immutable blockchain ledger, the proposed system delivers fully automated, cryptographically-guaranteed tamper detection that is robust against both classical and quantum-computing-based adversarial attacks.

The framework substantially reduces dependence on manual expert investigation, improves tamper detection accuracy, and produces a complete, legally admissible audit trail. Its lightweight architecture imposes minimal computational overhead, making it equally suitable for resource-constrained edge deployments and high-throughput cloud-based forensic platforms. Experimental outcomes confirm that the system reliably distinguishes authentic evidence files from tampered ones in real time.

VIII. FUTURE ENHANCEMENTS

Future work will target seamless integration with established forensic platforms such as Autopsy and The Sleuth Kit. Scalability to distributed multi-cloud environments using Hyperledger Fabric or Ethereum smart contracts is planned. Explainable AI (XAI) techniques — including SHAP value analysis — will be incorporated to generate humaninterpretable forensic reports. Real-world deployment and longitudinal validation within a Security Operations Centre (SOC) environment, augmented with MITRE ATT&CK threatintelligence feeds, is also envisioned.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506125|

REFERENCES

1. Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. *Int. Workshop on PostQuantum Cryptography (PQCrypto)*, Springer, LNCS 7071.
2. McGrew, D., Curcio, M., & Fluhrer, S. (2019). Leighton-Micali Hash-Based Signatures.
3. *IETF RFC 8554*. Internet Engineering Task Force.
4. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper*. Available: https://bitcoin.org/bitcoin.pdf
5. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Academic Press, Elsevier.
6. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, vol. 78, pp. 544–546.
7. Bonomi, S., Martines, M., Pejo, B., & Ruini, F. (2018). Blockchain-based Logging for the Cross-border Exchange of Digital Evidence. *Proc. 13th Int. Conf. on Availability, Reliability and Security (ARES)*. ACM.
8. Stelly, C., & Roussev, V. (2017). SCARF: A Container-based Approach to Cloud-Scale Digital Forensic Processing. *Digital Investigation*, vol. 22, pp. S39–S47, Elsevier.
9. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A Comprehensive
10. Analysis of the Role of AI and ML in Modern Digital Forensics and Incident Response.
11. *Forensic Sci. Int.: Digital Investigation*, vol. 48, Elsevier.
12. NIST. (2022). Post-Quantum Cryptography Standardisation. National Institute of Standards and Technology. Available: https://csrc.nist.gov/projects/post-quantumcryptography
13. Garfinkel, S. L. (2010). Digital Forensics Research: The Next 10 Years. *Digital Investigation*, vol. 7, suppl., pp. S64–S73, Elsevier.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details