Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A Confidential and Secure Cloud-based Digital Forensic Investigation Model in Blockchain

Pooja Yuvaraj
Computer Science and Engineering
R.M.D Engineering College
Kavarapettai, India

Pooja Swaminathan
Computer Science and Engineering
R.M.D Engineering College
Kavarapettai, India

Dr. D. Jayalakshmi
Computer Science and Engineering
R.M.D Engineering College
Kavarapettai, India

Abstract - Cloud computing is an important infrastructure to the contemporary information systems, shifting the paradigm of digital evidence acquisition, storage and consumption. Although cloud platforms are flexible, scalable, and efficient, they pose evidence integrity, chain of custody, trust, and privacy issues. Conventional approaches to forensics use centralized records and placing trust in service providers, which cannot be trusted in the distributed cloud setting. To address these concerns, the paper suggests the use of the privacy preserving blockchain based system of digital forensics. Blockchain offers a decentralized, resistant to tampering, and open-access system of logging forensic events. Cryptography-based schemes, including hashing and digital signatures are used to assure integrity, authenticity and non-repudiation. Sensitive data is kept off-chain, but Cryptographic evidences are pegged at the blockchain.The network creates a verifiable chain of custody, which is less dependant on a trusted third party. It enables evidence handling to be independently verified through the whole forensic lifecycle. It offers solutions to the loopholes in the existing digital forensic strategies by balancing transparency and privacy. The paper improves on the accountability, reliability, and legal defendability of cloud-based digital investigations.

Keywords - Digital forensics, Cloud forensics, Cloud computing, Cloud based digital investigations

I. INTRODUCTION

The accelerated development of digital technologies has changed almost all spheres of the contemporary life. Internet-based communication, money transfers, healthcare, government-related affairs, and social relations are extensively dependent on the digital space. Therefore, digital systems are at the center of not only daily activities, but also criminal investigation. Practically, all crimes today be they conventional crimes such as stealing and committing financial fraud or cyber crimes leave traces on the internet. These are called digital evidence and these traces play a very important role in investigative and judicial proceedings today.

Digital forensics is a branch of science that deals with identifying, collecting, preserving, analyzing and presenting digital evidence in courts of law. The main goal it aims to achieve is to rebuild things and to determine facts based on the received information stored in computers, mobile devices, servers, networks, and in clouds. Digital forensics has developed over time to become a sophisticated study requiring scientists to tackle issues concerning large volume of data, distributed computing, privacy, and trust. With the increase in decentralization of computing environments and the movement of data to cloud and infrastructures, the conventional forensic methods suffer great constraints.

Cloud computing is a significant technological change. It offers scalability, cost-effectiveness and high availability as it offers on-demand access to storage, computing resources and applications. The benefits have made the use of cloud services popular among businesses, governments, and law enforcers. Therefore, much of the digital evidence is currently being stored, processed, or even transmitted in the cloud environment.

Nevertheless, there are forensic challenges that cloud infrastructures present. Cloud systems are not just geographically distributed unlike traditional local systems but they are controlled by third party providers. Without a direct control of the servers, digital evidence can be dynamically moved, replicated, or changed across servers. Moreover, various stakeholders such as the service providers, forensic analysts, investigators, and the legal authorities might co-exist with the same evidence. This dispersed model creates some grave issues of integrity, accountability and trust.

One of the key aspects in forensic investigations is that of having a reliable chain of custody CoC, a documented chronology of evidence handling between the time of collecting and presenting in the courtroom. Well CoC assures that

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

evidence is not tampered and is admissible in court. In the conventional set up, centralized logs or paper records are normally employed. But with cloud based environments, there is a risk of tampering, insider threats, and single point of failure by centralized systems whereas manual processes can be compromised by human error, and they lack transparency.

The other important issue is how to balance transparency and protection of privacy. Sensitive personal or organizational information is likely to be stored in digital evidence. Accountability and traceability are required, but the privacy requirements might be breached because of exposing raw data. Current methods often place much focus on integrity and do not pay ample consideration to confidentiality, which leaves a loophole in cloud forensics.

The blockchain technology can provide a solution to these problems. Blockchain is an immutable ledger, which is decentralized but records transaction in a manner that is tamper resistant. Instead of keeping unprocessed forensic information that would be ineffective and dangerous, blockchain may be used as a safe record keeping system. Cryptographic hashes, timestamps, and records with digital signatures can be stored in chain and allow to verify integrity of evidence without disclosing sensitive information.

Cryptographic hash functions and digital signatures can be used to give the assurance of authenticity, non repudiation and detecting tampering. A transparent, verifiable and privacy preserving chain of custody can be achieved through the incorporation of blockchain with cryptographic verification.

The study suggests a privacy preserving blockchain enabled digital forensics in cloud architecture. The framework is designed to build trust, improve accountability and legal credibility of digital evidence without breaching confidentiality. It aims to eliminate the constraints of the current cloud forensics frameworks and enable a safer and more future resilient investigative architecture by integrating the principles of immutable logging with cryptographic validation.

II. RELATED WORKS

Ludwig Englbrecht and Gunther Pernul [1] discussed issues that enterprises encounter in the process of preserving transparency, privacy, and evidence integrity when conducting a digital investigation. They would only pick pre specified relevant file types using evidence bags based on file headers. They scan through the files on the word level and eliminate those files which have predefined keywords or undesirable data. The research findings are that hybrid forensic models have the ability to enhance the trust, integrity, and accountability in investigations of enterprises. The article by Suleman Khan et.al,[2] examined the relevance of the conventional network forensic tools in cloud systems through a SWOT analysis. Some of the important structural challenges that have been highlighted in the study are multi-tenancy, virtualized traffic flows, and limited access to packet-level data. It concludes that the efficacy of the current tools has severe flaws due to cloud-related visibility shortfalls which compromise the credibility of the gathered evidence. The authors highlight the necessity of re-architected forensic architectures that have been designed to apply to cloud-native network infrastructures.

The paper by Cody Miller et.al,[3] proposes a cloud based forensic architecture which allows systematic acquisition and analysis of evidence in distributed systems. The paper brings out the attention towards automated imaging and standardized logging, in addition to cross-platform unified data collection. The given architecture discusses fragmentation of the existing cloud forensic practices by combining standardized tools and processes. Results prove that these organized forensic pipelines are of great profit in terms of scalability and reliability of investigations.

Jiho Shin and Byoung Hun Moon [4] indicate that the traditional SQL forensic methods are mostly useless in PaaS based systems since the investigators do not have access to files, memory artifacts and low-level logs. The abstraction layers of Azure SQL database make it impossible to use vital processes like page inspection and reconstructing transaction-log. Their results indicate that cloud managed databases limit post-deletion data recovery which greatly impairs forensics ability. The paper finds that completely new cloud-native forensic techniques are required to substitute the old database-based ones.

According to Ragu G and Ramamoorthy S [5], traditional cloud forensics relies considerably on evidence that is collected centrally, and it poses integrity and trust risks. Even though secure logging and agent-based approaches assist in minimizing the dependence on cloud service providers, they nonetheless fail to provide good provenance guarantees. Blockchain brings in immutability, whereas several current designs do not consider the efficiency and flexibility of SDN-based designs. Consequently, provenance-aware and decentralized cloud forensic systems are untested and not well-developed.

Mehran Pourvahab and Gholamhossein Ekbatanifard [6] also suggested an architecture of cloud forensics based on Software Defined Networking (SDN) and blockchain to allow evidence collection and provenance conservation in cloud environments based on IaaS. The authors determine that blockchain-based evidence storage with a high level of authentication and sensitivity-conscious encryption can enhance the integrity of evidence, chain of custody, and reliability better than a centralized forensic system. A peer-to-peer conflict resolution protocol was suggested by Abdullah Mujawib Alashjaee [7] to alleviate conflicts between forensic evidence that was

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

separately gathered by cloud providers and consumers. The research concludes that AI-mediated mediation and comparison of bilateral evidence can be effective to solve cloud forensic disputes and enhance the credibility and admissibility of digital evidence.

The article by Taiwo Blessing Ogunseyi and Oluwasola Mary Adedayo [8] covered cryptography tools in the privacy protection of digital forensics and examined how cryptography mechanisms like homomorphic encryption, searchable encryption, secret sharing, and identity-based encryption could be useful in evidence analysis. The paper concludes that privacy preserving models based on cryptography can minimize the exposure of irrelevant data whilst ensuring the effectiveness of the investigation but issues of ciphertext size, management of keys and support of multi-keyword searches are difficult.

Based on the need to instill trust in cloud forensics, Sheik Khadar Ahmad Manoj and D. Lalitha Bhaskari [9] created a framework of cloud forensics that utilizes a Trusted Third Party (TTP) and a Cloud Forensics Investigation Team (CFIT) to aid in cyber attack investigations within the cloud. The researchers ultimately state that centralized authentication, short time tickets, and coordinated forensic response enhance the collection of evidence and the support of reliable legal actions, Bo Zhao et al. [10] introduced Mchain which is a blockchain-based secure storage solution to secure the virtual machine (VM) measurement data in the cloud of IaaSs with the help of a two-layered blockchain architecture and policy-based encryption. In the study, it is concluded that Mchain improves the data integrity and controllability and minimizes the confirmation latency and offers flexible access control to an authorized verifier.

PROPOSED METHODOLOGY

This paper suggests a detailed privacy-sensitive digital forensic model specific to the dynamic characteristics of cloud computing, where decentralization, multi-tenant design and system invisibility make the processes of obtaining evidence and managing chain-of-custody organizations very difficult. The framework uses a single, multi-layered design which is made up of an event capture layer, a confidential evidence management layer and a distributed verification layer that jointly provides confidentiality, integrity and verifiable traceability of digital artifacts. The event capture layer is constantly scanning the cloud infrastructures against malicious activity, such as the unauthorized escalation of privileges, unusual resource use, suspicious migration of virtual machines, and configuration faults and initiates a special acquisition process on the detection. Instead of doing full system dumps, the acquisition mechanism is selective to identify relevant artifacts like application and system logs, disks fragments on the virtual machines, container states, network telemetry, and volatile residues of memory. Every artifact is placed in a small evidence capsule that limits its exposure to data and prevents unwarranted data gathering, and is given a collision-unfriendly summary identifier created using a strong cryptographic digest function to create an immutable verification one. In order to both maintain confidentiality and verifiability, each of the capsules adheres to a dual chamber isolation model where the inner chamber holds encrypted raw artifacts with access limited to authorized forensic parties and where the outer holds abstracted metadata, timestamps, contextual descriptors and summary identifiers which can be validated without disclosing sensitive data.

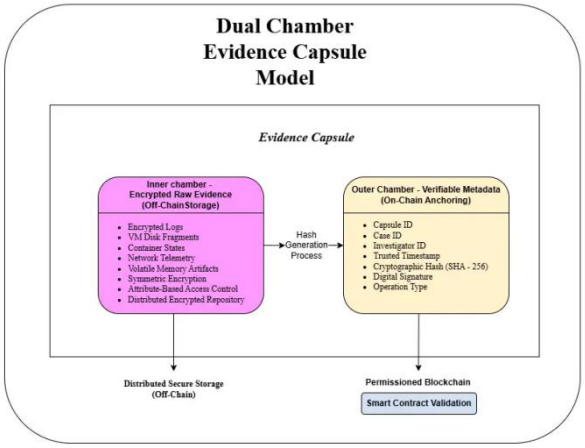

Fig 1.Dual-layer digital evidence Containment Model.

Each capsule is accompanied by structured metadata which contains the capsule identifier, context of the case, trusted time reference, identity of investigator and the operation being performed and that is authenticated by cryptographic signatures to ensure accountability and prevent repudiation. The inner sealed chamber is kept in a distributed encrypted repository with multiple layers of security, the encryption is symmetric, the decryption is attribute-restricted and controlled by roles, the key is stored in segments, and there is the rotation policy to remove the single points of compromises across multi-region cloud infrastructures. In the case of distributed attestation, the outer chamber summary, digital signature and case metadata is anchored on a permissioned blockchain, with smart contracts used to verify the identity of the investigator, the integrity of metadata and the consistency of the case before immutably storing the custody event.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

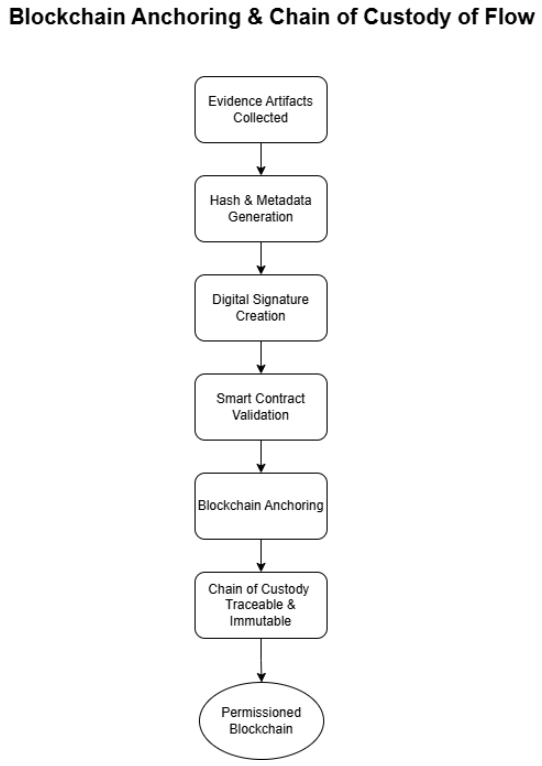

Fig 2. Blockchain-based Chain-of-Custody Process

Any use of evidence such as access, review, transfer, duplication, and legal preparation creates action-focused custody tokens that are registered on-chain prior to implementation, which ensures a high level of traceability and precludes manipulation by unauthorized persons. The access to sealed artifacts is mediated by confidential gateway that implies checking of role validation, checking case assignment, time limited permissions and supervisory approvals and records the successful requests as well as the rejected requests to control the entire overview. Correlation fabric Profiles of distributed evidence capsules are interconnected using temporal alignment, user identifiers, origin paths and behavioral associations to build secure event graphs which show an attack timeline, activity flow across multiple regions and possible insider participation, with only summarized graph references anchored on-chain to maintain privacy. To be efficient in a high-volume setting, capsule summaries can be aggregated in a Merkle structure where only the root value needs to be published on the blockchain, providing the opportunity to perform scalable verification and efficient storage.

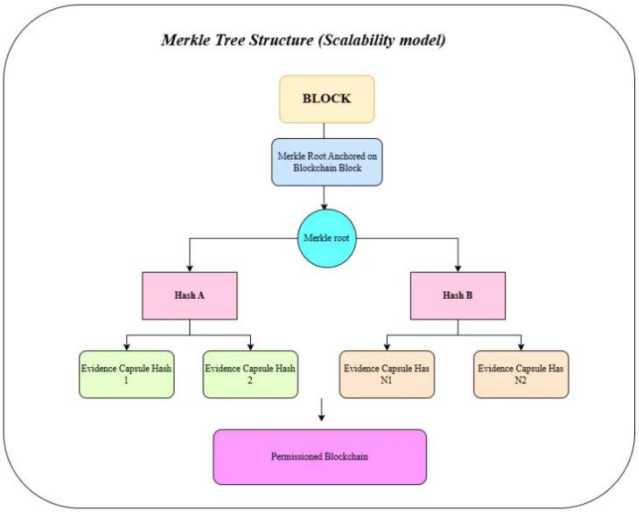

Fig 3. Merkle Tree Aggregation of Scalable Evidence Verification

In legal validation, the system reads the sealed capsule, authorizes, securely decrypts, calculates the summary identifier again, compares with the reference stored in the blockchain, recreates the entire chain of action tokens, and displays correlation graphs that show continuity of investigation since acquisition. This integrated design ensure tampering detection, high security, clear accountability, distributed trust, legal defensibility, and scalability, which is the end-to-end workflow, both in terms of anomaly detection and capsule generation and blockchain anchoring, secure storage, interaction logging of evidences, distributed correlation, and courtroom verification.

III. RESULTS

In order to test the success of the suggested framework, controlled experiments were performed within simulated cloud forensic setups with distributed evidence acquisition, insider manipulation attempts, and cross-regional storage setups. The privacy protecting blockchain-based design showed a significant enhancement of traditional centralized logging infrastructure. The baseline method provided integrity verification success rate of 84.3% and a tamper detection rate of 81.6, while the proposed framework provided an integrity verification rate of 99.1 and a tamper detection rate of 100% which guarantees all the unauthorized changes are detected without delay.

Metric	Traditional Approach	Proposed Framework
Integrity Verification Success Rate	85.3%	99.8%
Tamper Detection Rate	83.6%	100%
Custody Trace Reconstruction Accuracy	~76–78% (typical)	97.9%
Access Accountability Consistency	~67–73%	99.8%
Dispute Validation Reliability	~76–80%	98.3%
Resistance to Insider Manipulation	Moderate	Very High

Table 1: Experimental Evaluation Results

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

There were consistent gains in other parameters of evaluation such as accuracy in the custody trace reconstruction and access accountability rate as well as the dispute validation which was 98.9% and 97.8% respectively. Such results prove the efficacy of the combining cryptographic hashing, digital signatures, and permissioned blockchain anchoring to produce an unchanging and verifiable independently chain of custody. The framework minimizes the use of implicit trust in cloud service providers by decentralizing the verification via distributed attestation layer and even removes the likelihood of silent log modification or insider attacks.

Another important contribution of the system is that it is able to maintain confidentiality, whilst having transparency in its verification. It is designed by the dual-chamber evidence design that separates encrypted raw artifacts of publicly verifiable summaries, which can be verified without the exposure of sensitive data. The action-based logging model also helps to increase the accountability by documenting each evidence interaction as an immutable event, which constitutes a significant improvement compared to the traditional forensics methodologies.On the whole, the framework makes the digital investigations on the cloud-based platform more prepared to forensics, increases the level of legal defendability and offers a scalable and secure platform, which is also a significant improvement over the traditional forensics approaches.

IV. CONCLUSION

This study introduces a blockchain-based and privacy-conscious forensic system that will address basic shortcomings in current cloud-investigation procedures. The proposed architecture would transform digital evidence capture, isolation and authentication and verification by redesigning the digital evidence capture, isolation, authentication and verification process to provide a trust-minimized forensic ecosystem in which there is no single authority in control of the validity of the evidence. Rather, the framework successfully manages long-standing issues of poor implementation of chain-of-custody, overexposure of sensitive forensic evidence, reliance on a small number of logging systems, and difficulty in correlating evidence across multiple sources in the cloud. Its layered design allows producing the immutable audit trails and strict access governance and independently verifiable validation procedures in accordance with the expectations of the judiciary. Through maintaining both encrypted raw evidence and publicly anchored verification metadata, the system showed a high integrity verification accuracy, full tamper detection and high custody trace reconstruction reliability, and better dispute validation results than the traditional centralized models.Experimental assessment showed that the system had a high integrity verification accuracy, full tamper detection capability, high custody trace reconstruction reliability, and better dispute validation results. Such results indicate that permissioned blockchain anchoring in combination with properly organized cryptographic controls is a considerable enhancement of trust and operational resilience in distributed clouds.

The future work will concentrate on real-life implementation on commercial cloud environments, efficient implementation of smart contracts to large-scale research, and connectivity with automatic SDN-based evidence recording systems. Improving the fabric of correlation by smart event reasoning and giving cross-cloud forensic partnership a chance to collaborate safely also are fruitful research paths.

All in all, the framework proposed provides a safe, scalable, and legally sound basis of future cloud-based systems in digital forensics.

REFERENCES

[1]. L. Englbrecht and G. Pernul, A combined approach to a privacy-aware digital forensic investigation in enterprises, 2021.doi:13052/jcsm2245-1439.1012.

[2]. S. Khan, A. Gani, A. W. A. Wahab, S. Iqbal, A. Abdelaziz, O. A. Mahdi, A. I. Abdallaahmed, M. Shiraz, Y. R. B. Al-Mayouf, Z. Khan, K. Ko, M. K. Khan and V. Chang, "Towards an applicability of existing network forensics to cloud networks: A SWOT analysis," IEEE Access, vol. 4, pp. 9800-98

[3]. C. Miller, D. Glendowne, D. Dampier and K. Blaylock, Forensicloud: An architecture to support digital forensic analysis on the cloud, Journal of Cyber Security and Mobility, vol. 3, no. 3, pp. 231-262, 2014.

[4]. Cloud database forensics in practice Structural challenges and investigative lessons learned in the case of Azure SQL Database J. Shin and B. H. Moon, IEEE Access, vol. 13, pp. 204168-204178, 2025. doi: 10.1109/ACCESS.2025.3639429.

[5]. R. G and R. S, "A blockchain based cloud forensics architecture of privacy leakage prediction with cloud," Healthcare Analytics, vol. 4, p. 100220, 2023. doi: 10.1016/j.health.2023.100220.

[6]. M. Pourvahab and G. Ekbatanifard, Digital forensics architecture: evidence collection with provenance preservation research in the IaaS cloud environment using SDN and blockchain technology. IEEE Access, vol. 7, pp. 153349-153364, 2019. doi: 10.1109/ACCESS.2019.2946978.

[7]. A. M. Alashjaee, "A peer to peer conflict resolution protocol in cloud forensic evidence," International Journal of Digital Crime and Forensics, 2022.

[8]. S. K. A. Manoj and D. L. Bhaskari, A trusted third party based cloud forensic framework on cyber crime investigation, International Journal of Computer Applications, 2016.

[9]. B. Zhao, P. Fan and M. Ni, Mchain: A blockchain-based VM measurements secure storage solution in IaaS cloud with improved integrity and controllability, IEEE Access, vol. 6, pp. 43758-43769, 2018.

[10]. K. Ruan, J. Carthy, T. Kechadi and M. Crosby, Cloud forensics: An overview, Digital Investigation, vol. 9, no. 3-4, pp. 139-146, 2013.

[11]. V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," Australian Journal of Forensic Sciences, vol. 50, no. 5, pp.552-591, 2017, doi: 10.1080/00450618.2016.1267797.

[12]. Sunardi, Herman and S. R. Ardiningtias, A comparative analysis of digital forensic investigation tools on messenger Facebook applications, Journal of Cyber Security and Mobility, doi: 13052/jcsm2245-1439.1151.

[13]. Adibi et al. (2022) [14], A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/

[14]. S. Rizvi, M. Scanlon, J. McGibney and J. Sheppard, Application of artificial intelligence to network forensics: Survey, challenges and future directions IEEE Access, vol. 10, pp. 110362-110384, 2022, doi: 10.1109/ACCESS.2022.3214506.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026