Educational Administration: Theory and Practice
2024, 30(5), 5556-5564
ISSN: 2148-2403
https://kuey.net/
Research Article

Preservation Of Digital Forensic Evidence Using Blockchain Technology

S. Adolphine Shyni[1*], Dr.N. Palanivel[2], R.Soundariya[3], K.Subalakshmi[4], S.Sivasanker[5]

[1*]Assistant Professor CSE (IoT, Cyber Security including Blockchain Technology) Manakula Vinayagar Institute of Technology Puducherry, India. adolphine1996@gmail.com
[2]Associate Professor, Department of Computer Science and Engineeing Manakula Vinayagar Institute of Technology Puducherry, India. npalani76@gmail.com
[3]UG Scholar, CSE(IoT, Cyber Security including Blockchain Technology) Manakula Vinayagar Institute of Technology Puducherry, India. rajsoundariya@gmail.com
[4]UG Scholar, CSE (IoT, Cyber Security including Blockchain Technology) Manakula Vinayagar Institute of Technology Puducherry, India. subakaruna08@gmail.com
[5]UG Scholar, CSE(IoT, Cyber Security including Blockchain Technology) Manakula Vinayagar Institute of Technology Puducherry, India. sivasanker1703@gmail.com

Citation: S. Adolphine Shyni, et al (2024), Preservation Of Digital Forensic Evidence Using Blockchain Technology, *Educational Administration: Theory and Practice*, *30*(5), 5556-5564, Doi: 10.53555/kuey.v30i5.3821

ARTICLE INFO **ABSTRACT**

It is evident that safeguarding electronic evidence against various negative outcomes, like tampering or destruction, is crucial for preserving its integrity. To ensure that the evidence is sufficiently pure to be allowed into evidence in court and to protect the integrity of the system, we must take preemptive action against these and other instances. The sequential recording of documents is all that is required for Chain of Custody. A criminal investigator may adhere to all procedures specified in the Chain of Custody in order to guarantee the accuracy of the data. The Chain of Custody is significant because it is impossible to demonstrate that evidence was not altered between its collection and its use in court. As a result, the gathered evidence lacks credibility. Using blockchain technology, a decentralized network that generates a secure database by hashing and storing data in blocks, chain of custody can be implemented in an open and secure manner. We support the Chain of Custody procedure by using Ethereum-based blockchain technology, which helps to verify the accuracy of data submitted at the time of court submission and helps to monitor data access.

Keywords— Chain of custody, blockchain-based chain of custody, hashing and storing data, Ethereum based, Peer to peer, tamper proof

I. INTRODUCTION

The process of locating, looking into, keeping, evaluating, verifying, and presenting digital evidence in a way that is acceptable to the law is known as digital forensics or DF. Since digital evidence can be used to establish facts or find cybercriminals guilty, it is becoming more and more significant. The goal of digital forensics is to guarantee the admissibility of digital evidence in a court of law. For this reason, in 2 any forensic investigation, it is essential to preserve the integrity of digital evidence during its whole lifecycle.

Due to its inherent qualities such as ease of transmission, fragility, susceptibility to tampering and removal, defenselessness against alteration and deletion, and time sensitivity digital evidence is more difficult to handle and maintain than physical evidence. Digital forensics primarily centers on the Chain of Custody (CoC).

The Digital Chain of Custody (DCoC) is a procedural framework for handling digital evidence in investigations. It is employed from the initial incident to its presentation in court, ensuring the preservation and sequential documentation of digital evidence. This process involves the transfer of evidence through various stages of hierarchy, starting from the initial collector to the ultimate authority in the court system. CoC is a crucial step in the research process. Every little detail pertaining to the evidence is documented, including the five W's (who, what, when, where, and how) for every phase of the inquiry. CoC must be kept in good condition and be impenetrable in order to guarantee the admissibility of the evidence in tribunals. It is crucial to maintain the integrity of the evidence.

Managing digital evidence from the moment it is gathered until it is used as evidence in court is the aim of this paper. The evidence is handled by several people during this process, which raises the possibility of tampering. It is crucial to preserve integrity, authenticity, and security to guarantee tamper resistance.

II. LITERATURE SURVEY

A. Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry.

This article explores how blockchain technology affects airport supply chain management (SCM) and operations management (OM) for sustainable performance. Because blockchain technology facilitates information and data exchange, encourages stakeholder collaboration, and lessens fragmentation, the authors conclude that it has the potential to enhance OM and sustainability in supply chain management. They do point out, though, that managers and legislators must cooperate to establish a cooperative atmosphere characterized by a shared culture and mutual trust, and that the use of blockchain technology does not ensure the acquisition of optimal performance.

B. Blockchain-Based Multimedia Evidence Preservation Framework for Internet of Things: A Digital Chain of Custody

Smart gadgets have made daily chores easier and are now an essential part of people's routines thanks to the Internet of Things (IoT). As a result, services that depend on sharing personal information are becoming more prevalent in several areas, including home automation, healthcare, and agriculture. The likelihood of digital crimes rises with the number of smart gadgets. Because everyone leaves digital traces behind, digital forensics is useful when looking into crimes using the Internet of Things. This paper presents BEvPF-IoT, a blockchain-based evidence-preservation framework designed for Internet of Things devices, to safeguard digital artifacts and prevent tampering until they are produced in court. Experiments on a blockchain network are used to evaluate feasibility, with an emphasis on throughput, latency, and gas usage. The suggested paradigm guarantees trustworthy investigation outcomes by improving accountability and openness in digital multimedia evidence forensics.

C. A Privacy-Preserving Platform for Healthcare Data Based on Blockchain Technology

Healthcare data has recently piqued the interest of cybercriminals. Decentralization could lessen the disastrous consequences of medical data. Peer-to-peer (P2P) networks facilitate decentralization, enabling several parties to securely store and handle private health data. Distributed or decentralized procedures are used by blockchain technology to ensure the accountability and integrity of its use. With the use of blockchain technology, this study offers a patient-centered healthcare data management system that stores data anonymously. Pseudonymity is guaranteed by the use of cryptographic techniques to protect patient data.

D. Digital Forensics using blockchain

It is clear from thinking about the integrity of electronic evidence that protecting it from unfavorable consequences—like change or destruction—is essential. To preserve system integrity and ensure the integrity of evidence that is admitted into evidence in court, protection against these and other occurrences is required. A series of processes that criminal investigators must follow to ensure the accuracy of information is included in the Chain of Custody, a chronological record-keeping system. Its importance rests in making sure that evidence is collected and presented in court without alteration; if it isn't, the evidence won't be credible. Data hashing and block storage are two methods used by blockchain technology, a decentralized network used by cryptocurrencies like Bitcoin, to guarantee a safe database.

III. PROBLEM STATEMENT

Present-day forensic techniques for digital evidence storage mainly depend on centralized systems such as cloud storage and databases. These have significant disadvantages despite providing advantages like scalable storage and organized storage. The integrity of the evidence may be compromised by centralized databases' susceptibility to single points of failure and data breaches. Cloud storage raises questions about data ownership, privacy, and legal ramifications with third-party suppliers. A secure, decentralized method for storing digital evidence is required to get around these restrictions. Enhancing security via tamper-proof storage, better scalability to manage increasing evidence quantities, investigator-defined data ownership and control, and visible audit trails to guarantee the admissibility of evidence should be the top priorities of this system. Advanced encryption methods, decentralized file systems, and blockchain technology are some potential remedies.

IV. OBJECTIVE

To improve digital evidence's security, integrity, and traceability, a blockchain-based digital forensic evidence storage initiative is being undertaken. Traditional approaches to maintaining digital evidence have shortcomings that blockchain's unique features—immutability, transparency, and decentralization—can help with.

V. EXISTING SYSTEM

Existing systems for storing digital evidence in digital forensics primarily rely on centralized databases and cloud storage solutions. Centralized databases, such as relational databases (RDBMS) and NoSQL databases, are commonly used to store digital evidence. While these databases offer structured storage and efficient querying capabilities, they are susceptible to single points of failure and security breaches. Unauthorized access or data corruption could compromise the integrity of the stored evidence.

Cloud storage solutions are scalable and affordable cloud storage for massive volumes of digital evidence offered by cloud storage solutions like Microsoft Azure Blob Storage and Amazon S3. However, cloud storage introduces concerns about data privacy and control. Relying on third-party cloud providers raises security risks and potential legal issues regarding data ownership and access.

A. *Existing architecture*

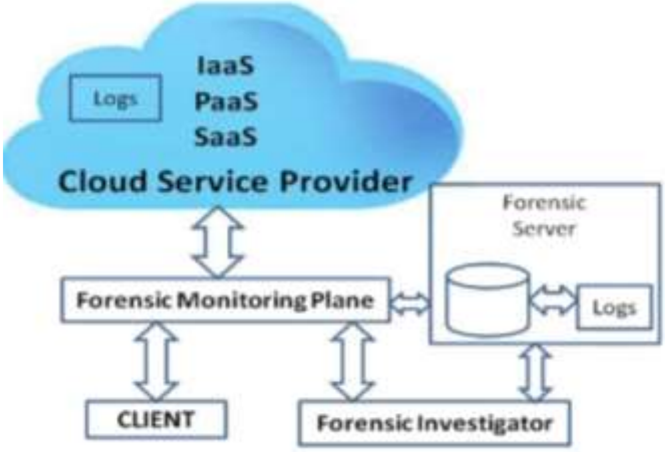


Fig. 1

VI. DRAWBACKS OF AN EXISTING SYSTEM

A. *Security flaws in centralized databases*

1) *Single point of failure:* All data kept on the database server may be jeopardized by a cyberattack or other system malfunction.
2) *Insider threats:* A cyberattack or other system error might compromise all of the data stored on the database server.
3) *Physical security issues:* Physical security is necessary to prevent theft and unauthorized access to database servers.
4) *regulatory risks:* Regulations may limit the storage and transfer of digital evidence by third-party services, depending on the jurisdiction.

B. *Cloud Data Storage*

1) *Data privacy:* Cloud service providers have the capacity to collect and analyze user data, which might lead to concerns about privacy regarding personal data.
2) *Dependency on outside vendors:* Evidence stored on cloud servers is no longer under the investigators' control in terms of its location or security.
3) *Vendor lock-in:* It may be costly and challenging to move cloud providers when dealing with a large amount of evidence.
4) *Scalability issues:* Conventional databases may find it challenging to organize and store vast quantities of diverse digital evidence.

VII. PROPOSED SYSTEM

Digital evidence can be managed in a safe, transparent, and unchangeable manner with the help of the suggested blockchain-based CoC system for digital forensic evidence. The solution uses smart contracts and an online application to support the CoC policy, trace all transfers of digital evidence, and verify the identities of all persons involved. The CoC records are stored on a distributed ledger called the blockchain, which is extremely difficult to hack. The system is hence immune to manipulation and unauthorized entry. This technology also ensures the integrity of digital evidence by maintaining a tamper-proof record of any adjustments made to the evidence on the blockchain. It is therefore very difficult to change the evidence without being noticed. The system also provides an audit trail.

VIII. METHODOLOGY

A. *Blockchain*

The blockchain is a growing entry-level database. With the invention of Bitcoin in 2008, the blockchain saw a transformation. It is something that is expected to have an impact on every business, including the legal, media, political, and artistic sectors in addition to the financial sector. Peer-to-peer systems include several participants, referred to as nodes, who share the ledger or records. Subgroups of the blockchain can be distinguished based on whether network nodes need permission to act as validators. A safe hash of the timestamp, the current block, and the previous block is present in every block of the blockchain. Once Records are uploaded to the blockchain whenever someone tries to alter the hash value that is currently in effect.

B. *Chain of Custody*

- CoC is nothing more than a series of documents that list the physical or electronic evidence along with the analysis, transfer, control, and custody orders. Risky steps are included in the Code of Conduct for both the investigation and the courtroom evidence submission process.
- The CoC should be safeguarded against alterations made to the evidence post-collection. Consequently, it is crucial to store the evidence in a manner that prevents tampering, ensuring easy presentation to the court without any doubts regarding its authenticity.

C. *Step involved*

1) *Locating and Gathering Electronic Proof:* Finding and gathering digital evidence pertinent to a cybersecurity incident, legal case, or investigation is crucial before utilizing blockchain technology. Files, logs, emails, and any other digital data that is relevant to the investigation's context can be included as evidence.
2) *Digital Evidence Hashing:* Hashing the gathered digital evidence is the next step. After applying a hash function to the data, the result is a fixed-length character string that is referred to as the digest or hash value. The original data is uniquely represented by this hash value. The hash value is a useful tool for identifying changes because it changes significantly even with small changes in the data.
3) *Keeping the Blockchain Hash Stored:* The blockchain is then used to store the hash value that was generated. This hash is publicly recorded on a distributed, decentralized ledger in a public blockchain. It is incorporated into a network to which only individuals with permission are able to access a private blockchain. Information about the evidence, its metadata, the recording timestamp, and any pertinent case or investigation details are usually included in the blockchain entry.
4) *Chronological Order Timestamping:* A timestamp that indicates the precise moment the evidence was added to the blockchain is appended to every entry on the blockchain. The chronological order and integrity of the evidence are guaranteed to be preserved by this timestamp. It is essential to establishing the custody chain.
5) *Utilizing Smart Contracts for Automated Evidence Management:* Smart contracts, which are self-executing contracts with established rules, can be used to automate evidence-processing processes. For instance, under specific circumstances, a smart contract can trigger actions such as the submission, verification, or release of evidence. The assures uniform, unchangeable evidence handling and lowers the chance of human mistakes.

IX. ALGORITHM

A. *Hashing*

On the blockchain, hash functions are essential to the preservation of digital evidence. The digital evidence is fed into a hash function, which outputs a fixed-length character string called a hash value or digest. Due to the deterministic nature of this process, the same input will consistently yield the same hash value. Additionally, hash functions are designed to be irreversible, making it computationally impossible to retrieve the original input from the hash value.

B. *Smart Contract*

Smart contracts are crucial for automating the handling of evidence, even though they are not cryptographic algorithms in the conventional sense. Self-executing contracts with pre-established terms and conditions are known as smart contracts. By making it easier to submit, verify, and release evidence in accordance with predetermined standards, they lower the possibility of human error and guarantee reliable and consistent evidence management. Smart contracts in blockchain systems such as Ethereum are written in Solidity, a programming language created especially for safe, decentralized application development.

1) *Contract Declaration:* The blockchain-based EvidenceContract ensures the digital evidence's

X. SYSTEM ARCHITECTURE

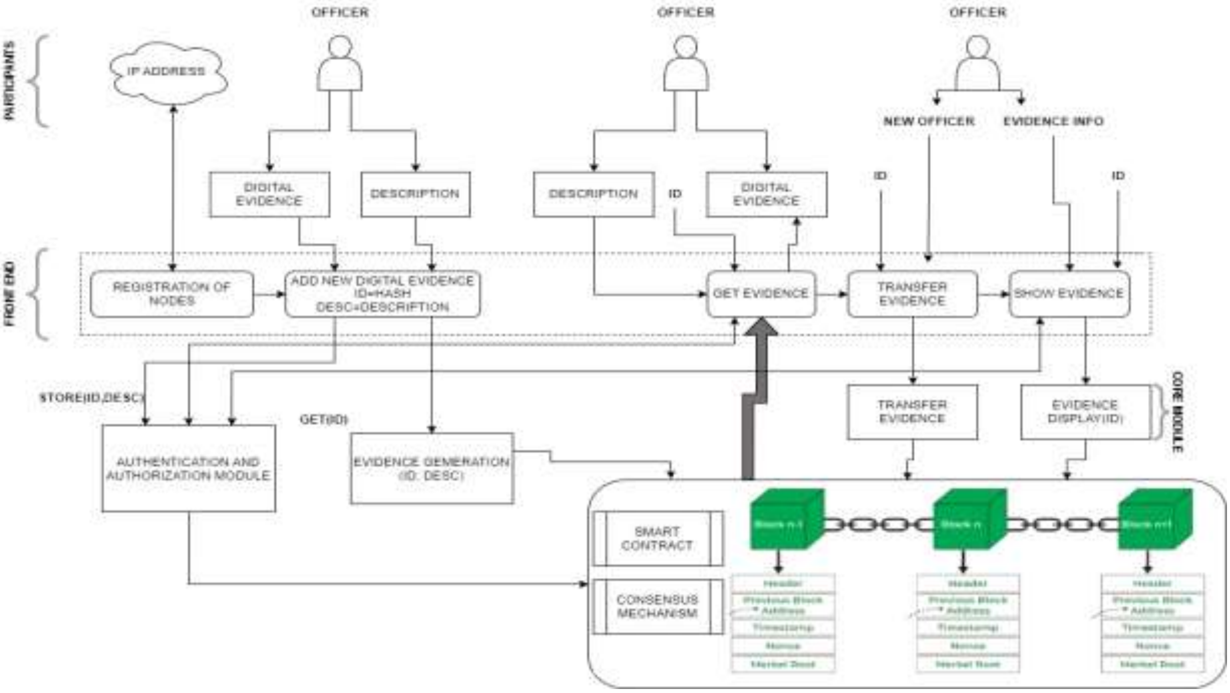


Fig. 2. Proposed system architecture

integrity and immutability while streamlining the submission and verification procedure.

2) *Data Structure:* A structure for evidence submission is defined in the contract.

a) *User:* Keeps track of the Ethereum address of the evidence-submitting user.

b) *Data Hash:* Protects the digital evidence's SHA-256 hash, guaranteeing its integrity.

c) *Timestamp:* Keeps track of the precise moment (block time) at which the evidence was delivered.

3) *Event Recording:* Evidence submissions that are successful are tracked by the contract using an Evidence Submitted. This event captures:

a) User address of the submitted.

b) Hash of the submitted evidence.

c) Timestamp of the evidence submission.

4) *Submitting Evidence:* Users can submit digital evidence for safe blockchain storage using the Submit Evidence function.

a) *Unique Identifier:* The function hashes the user address, the hash of the evidence, and the current block timestamp to provide a unique identity for the evidence.

b) *Duplicate Check:* The unique identification is used by the system to confirm if the evidence has previously been submitted. Entries that are submitted twice are rejected.

c) *Evidence Storage:* The user address, proof hash, and timestamp are recorded on the blockchain utilizing the unique identification as a point of reference if the evidence is unique.

d) *Event Emission:* The Evidence Submitted event is released, documenting the submission information, upon successful submission.

5) *Verifying Evidence:* By utilizing its hash, the verify Evidence function enables users to verify the presence of certain evidence.

a) *Unique Identifier Generation:* The user address and evidence hash are used to produce a unique identity, just like in submission.

b) *Evidence Retrieval:* The system makes an effort to access the blockchain maintain and extract the evidentiary information linked to the unique identification.

c) *Existence Check:* A "not found" error is raised if the hash supplied does not yield any evidence.

d) *Verification Success:* The user address (submitter) and submission timestamp are returned if there is proof of it.

XI. PERFORMANCE METRICS

By leveraging blockchain technology, the proposed effort aims to enhance the transparency and security of the Chain of Custody (CoC) process for digital evidence in court proceedings.

A. *Metrics for Security*

1) *Data Integrity:* The immutability of blockchain technology makes it impossible to tamper with evidence, which is one of its strengths. We may compute the Data Integrity Ratio (DIR) to put this into numerical form:

$$\text{DIR} = \frac{\text{Total number of hash verifications}}{\text{number of successful hash verifications}}$$

A DIR near 1 denotes a high degree of consistency between the evidence's recorded hash values and the original data, indicating that it is undisturbed

2) Efficiency of Access Control: Evidence integrity may be jeopardized by unauthorized access. We can use the formula to gauge this.

$$\text{Efficiency} = \frac{1 - (\text{Total number of access attempts})}{\text{number of unauthorized access attempts}}$$

B. *Metrics of Performance*

1) *Transaction Throughput (TPS):* Evidence submissions must be handled efficiently. The number of CoC transactions handled in a second is measured by TPS.

$$\text{TPS} = \frac{\text{Number of Completed CoC transactions}}{\text{Time interval(seconds)}}$$

Greater TPS suggests improved scalability to manage heavy workloads.

2) Latency: It's critical to obtain proof quickly. The average time taken by a CoC transaction (such as the submission of evidence) to be completed on the blockchain is measured by latency.

$$\text{L} = \text{Average Time for CoC Transaction Completion}$$

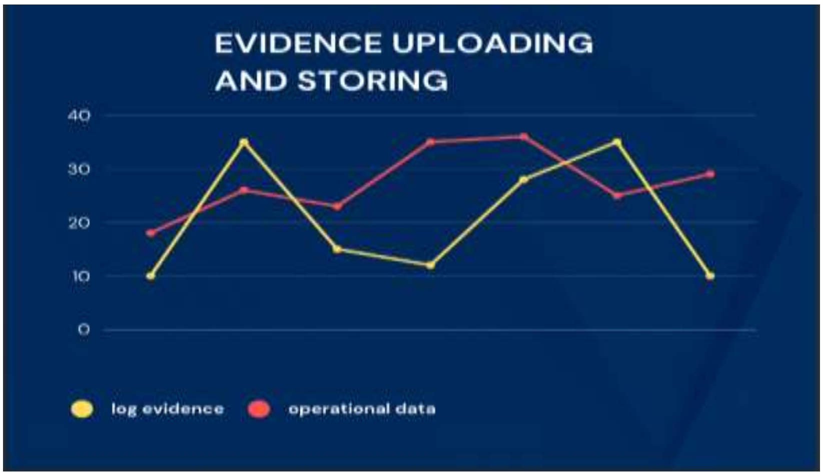


Fig. 3. Analysis of log evidence and operational data

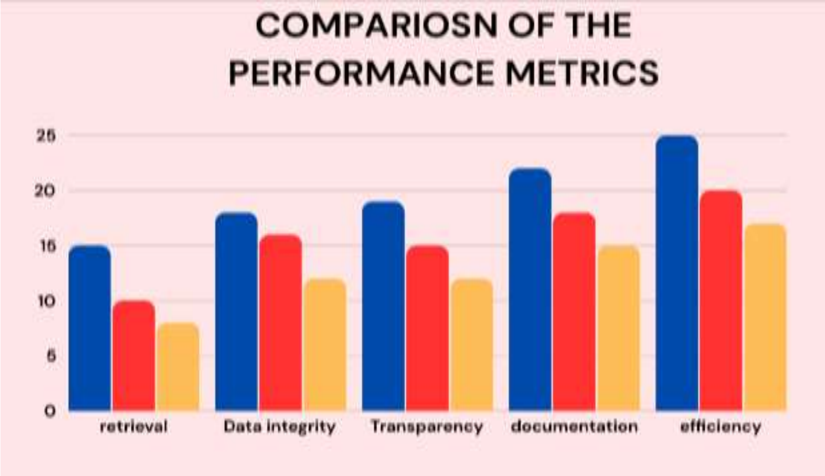


Fig.4. Comparison among cloud, database, blockchain

XII. EXPERIMENTAL RESULT

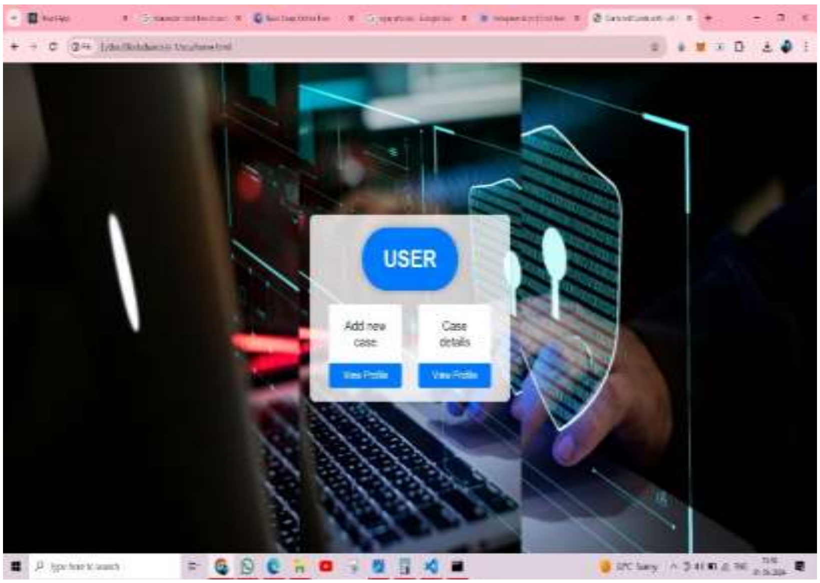


Fig.4. Home page

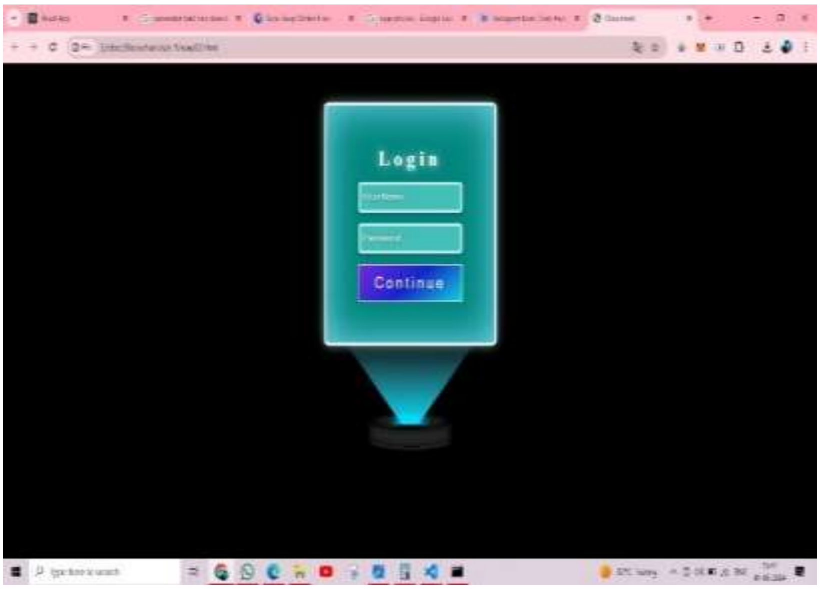


Fig.4. Login form for Officers

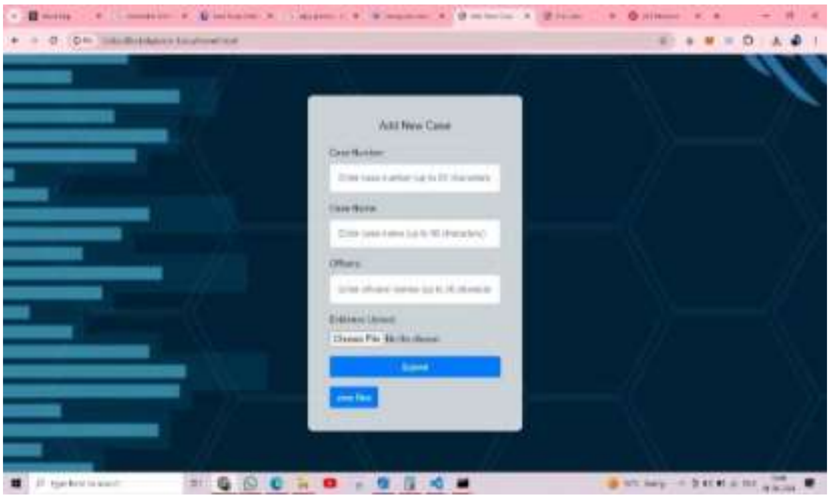
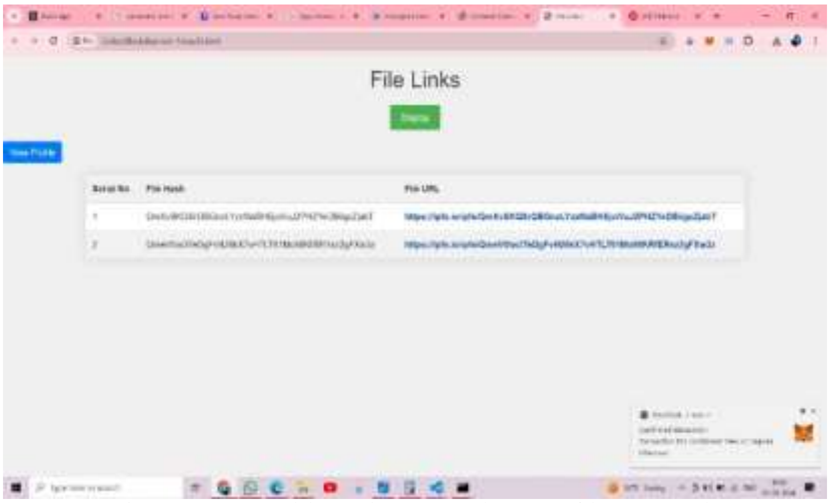


Fig.4. Case Dashboard to add the details of new cases



File Links

Serial No.	File Hash	File URL
1	[illegible]	[illegible]
2	[illegible]	[illegible]

Fig.4. User Dashboard to view the case files securely

XIII. CONCLUSION

This initiative offers a major development in protecting the reliability and confidentiality of digital data for forensic investigations and judicial procedures by incorporating blockchain technology. The paper builds a strong and safe basis for the safeguarding of digital evidence by utilizing the decentralized management, immutability, and transparency of the blockchain. The main issues with maintaining digital evidence are addressed by this suggested solution, which includes guarding against data alteration and illegal access. The resultant blockchain-based approach strengthens the credibility of digital evidence and safeguards the chain of custody, which could improve its admissibility in court. Beyond the field of digital forensics, this approach finds extensive use in secure communications, cybersecurity, and blockchain technologies, all of which significantly depend on data integrity. This paper demonstrates the transformative potential of blockchain technology by providing a potent solution to the problems of preserving and guaranteeing digital data integrity in today's increasingly digitalized world, where technology is constantly evolving and the importance of digital evidence in legal and investigative proceedings is rising. This creative solution offers a robust and reliable method for managing and believing digital evidence in our increasingly digital environment.

REFERENCE

1. G.Horsman, Unmanned aerial vehicles: a preliminary analysis of forensic challenges, Digit. Invest. 16 (2016) 1–11.
2. B.E. Koenig, Authentication of forensic audio recordings, J. Audio Eng. Soc. 38 (1/ 2) (1990) 3–33.
3. E.B. Brixen, Techniques for the authentication of digital audio recordings, in: Audio Engineering Society Convention 122, Audio Engineering Society, 2007, May.
4. T. Owen, AES recommended practice for forensic purposes-managing recorded audio materials intended for examination, J. Audio Eng. Soc. 44 (4) (1996) 275.
5. J.L. Barron, D.J. Fleet, S.S. Beauchemin, Performance of optical flow techniques, Int. J. Comput. Vis. 12 (1) (1994) 43–77.
6. A.J. Fridrich, B.D. Soukal, A.J. Luka’s, Detection of copy-move forgery in digital images, in: Proceedings of Digital Forensic Research Workshop, 2003.
7. S. Rani, Digital forensic models: a comparative analysis, Int. J. Manag. IT Eng. (IJMIE) 8 (6) (2018) 432–443.
8. S. Agarwal, H. Farid, Photo forensics from rounding artifacts, in: Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security, 2020, June, pp. 103–114.
9. K. Ghazinour, D.M. Vakharia, K.C. Kannaji, R. Satyakumar, A study on digital forensic tools, in: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), IEEE, 2017, September, pp. 3136–3142.
10. Tasatanattakool, P., &Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. In 2018 International Conference on Information Networking (ICOIN) (pp. 473-475). IEEE.
11. Flores, D. A., &Jhumka, A. (2017, August). Implementing Chain of Custody Requirements in Database Audit Records for Forensic Purposes. In 2017 IEEE Trustcom/BigDataSE/ICESS (pp. 675-682). IEEE.
12. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., &Amaba, B. (2017, June). Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (pp. 137-141). IEEE.
13. S.C. Sathe, N.M. Dongre, Data acquisition techniques in mobile forensics, in: 2018 2nd International Conference on Inventive Systems and Control (Icisc), IEEE, 2018, January, pp. 280–286.

14. Gautami Tripathi,Mohd Abdul Ahad,Gabriella Casalino A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges
15. Sanka and R. C. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” J. Netw. Comput. Appl., vol. 195, Dec. 2021, Art. no. 103232.
16. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, “Emerging trends in blockchain technology and applications: A review and outlook,” J. King Saud Univ. Comput. Inf. Sci.,
17. D. Kirli, B. Couraud, V. Robu, M. Salgado-Bravo, S. Norbu, M. Andoni, I. Antonopoulos, M. Negrete-Pincetic, D. Flynn, and A. Kiprakis, “Smart contracts in energy systems: A systematic review of fundamental approaches and implementations,” Renew. Sustain. Energy Rev., vol. 158, Apr. 2022, Art. no. 112013.