

EVIDENCE PROTECTION SYSTEM USING BLOCKCHAIN PRINCIPLES

Project Reference No.: 49S_BE_1323

College : Biluru Gurubasava Mahaswamiji Institute of Technology, Mudhol,
Bagalkot
Branch : Department of Computer Science and Engineering
Guides : Prof. Padmini P. Nandeppanavar
Prof. Navin M. Mathad
Students : Mr. Khabeer Hashim A. Chistipeera
Mr. Nayeem B Dindawar
Mr. Toupik Ainapur

Keywords:

Blockchain, Digital Evidence, SHA-256, IPFS, Data Integrity, Tamper-Proof System.

Introduction:

Digital evidence plays a vital role in modern investigations and legal processes. However, it is highly vulnerable to tampering, unauthorized access, and data manipulation. To address this, a secure and reliable system is required to ensure the integrity and authenticity of digital evidence. This project proposes an Evidence Protection System using blockchain principles, where SHA-256 hashing and chain linking techniques are used to detect any changes in the data.

The system ensures tamper-proof storage, maintains a transparent chain of custody, and improves trust in digital evidence handling.

Objectives:

- **To Ensure Data Integrity Using SHA-256 Hashing:** Generates a unique hash for each evidence file, ensuring even minor changes can be detected.
- **To Create an Immutable Blockchain-Based Evidence Chain:** Links each record with the previous one, making the chain tamper-proof and secure.
- **To Implement Secure Role-Based Access Control:** Restricts access based on user roles, allowing only authorized users to modify evidence.
- **To Maintain a Transparent Chain Of Custody:** Records all actions like upload, view, and verification with timestamps for traceability.
- **To Develop a User-Friendly Web Application:** Provides an easy interface for users to upload, access, and verify digital evidence.

Methodology:

The development of the Evidence Protection System using Blockchain Principles follows a simple and organized approach to ensure that digital evidence is handled securely and efficiently. The process starts with planning, where the goals of the project, its scope, and basic requirements are identified. After that, requirement analysis is carried out to understand what features the system should have and how it should perform.

Next comes the design phase, where the structure of the system, database, and security features like SHA-256 hashing and blockchain linking are planned. In the implementation phase, different modules such as user login, evidence upload, hash generation, and verification are developed using Flask and SQLite.

Once the system is developed, testing is done to check if everything works properly and securely. This includes checking for errors, performance issues, and security vulnerabilities. After successful testing, the system is deployed so that users can access it through a web interface. Finally, regular maintenance and updates are carried out to improve the system, fix any issues, and ensure it continues to work efficiently.

Result:

The Evidence Protection System using Blockchain Principles was successfully developed and tested. The system allows users to securely log in and manage digital evidence. When a file is uploaded, a unique SHA-256 hash is generated and stored, which helps in maintaining the integrity of the data. The system can easily detect any changes made to the evidence by comparing hash values. If the file is modified, the system immediately shows that it has been tampered with. The dashboard is simple and easy to use, allowing users to upload, view, search, and verify evidence without difficulty. Role-based access control ensures that only authorized users can make changes, while others can only view the data. Overall, the system works efficiently and provides a secure, reliable, and transparent way to manage digital evidence.

←

🔄

🌐 localhost:5000/evidence

🔍

🔖

🌟

⚙️

⋮

👤 Ch...

Summarize

🔗

🔍

🔖

🌟

⚙️

⋮

👤 Ch...

EvidenceChain

All Evidence

Verify Chain

Upload

Admin: Users

Logged in as: Nayeem D (authorized)

Logout

Evidence List

Search All Fields

Case ID

Uploader

Date From

Date To

Clear

Search evidence...

All Cases

All Uploaders

dd-mm-yyyy

dd-mm-yyyy

Showing 4 of 4 records

Case ID	Case Number	Case Name	Original Name	Stored File	File Hash	Prev Hash	Block Hash	Timestamp	Uploader	Notes	Document	
1	A1	1	car crash	car.jpg	2025122210334663726_car.jpg	41e8 538fa 49ab 29a2 b022 d4d1f 3788f 7faa4 afb92 9904 8e1b 1b32 78e5	GENE SIS	42ae8 fd912 7446f 5370c c8fee 07294 b11cb cf805 52c2c 5291d 55eca c712f	2025-12-22 11:03:34Z	 Nayeem D	car image	Download

Show details

Figure 1: Display of Uploaded Evidence Records with Blockchain Hash Details:

This screen displays all uploaded evidence along with SHA-256 hash values. Each hash uniquely represents a file and helps identify any tampering.

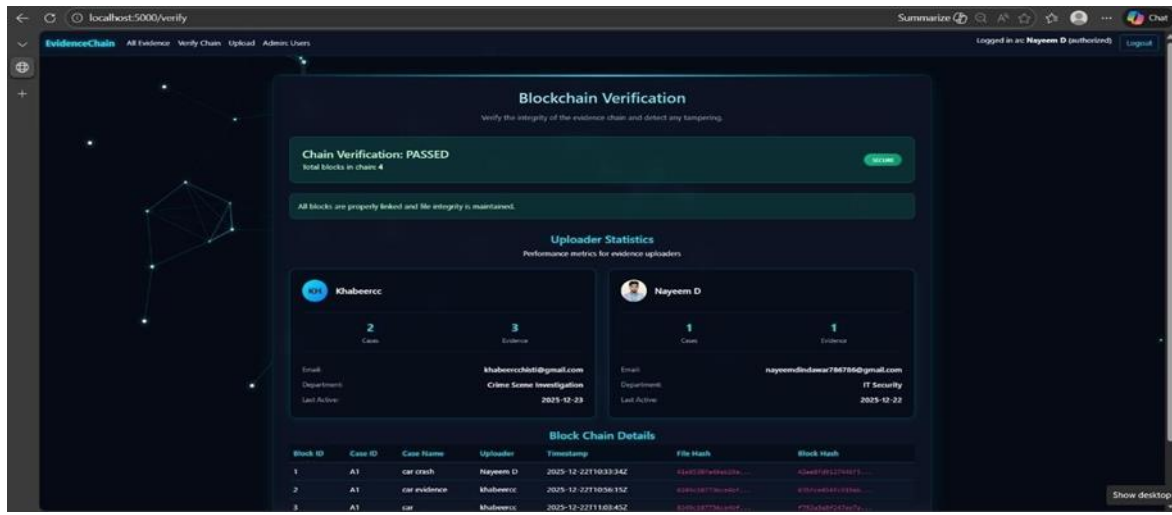


Figure 2: Blockchain Verification Interface of the Evidence Protection System:

This interface verifies evidence authenticity by recalculating file hashes. If the generated hash matches the stored hash, the evidence is considered secure.

Conclusion:

1. The Evidence Protection System using Blockchain Principles offers a simple and effective way to keep digital evidence safe and trustworthy. By using SHA-256 hashing and linking records like a chain, the system can easily detect if any data has been changed.
2. It also includes useful features like secure login, role-based access, and a clear record of all activities, which makes it easy to track and manage evidence. Overall, the system is easy to use, reliable, and helps improve the security and transparency of digital evidence handling.

Project Outcomes:

- The system provides a simple and secure way to manage digital evidence.
- SHA-256 hashing helps detect any changes in the evidence easily.
- Blockchain-based linking ensures data is tamper-proof and reliable.
- Role-based access control keeps the system safe from unauthorized users.
- The chain of custody is maintained clearly with proper tracking of activities.
- The user-friendly interface makes the system easy to use.
- Overall, the system improves security, transparency, and trust in digital evidence handling.

References:

1. [1] K. Verma and S. Rao, "Blockchain applications in cybersecurity and digital evidence management," *International Journal of Advanced Computer Science*, Jun. 2023.
2. [2] D. Sharma, R. Verma, and P. Gupta, "Blockchain for crime record management," *Journal of Digital Forensics and Cyber Security*, Aug. 2022.

3. [3] L. Zhao, T. Wu, and Y. Chen, "Decentralized data storage using blockchain," *IEEE Access*, Nov. 2022.
4. [4] M. Ahmed, S. Khan, and R. Ali, "Secure digital forensics using Hyperledger," in *Proceedings of the IEEE Cyber Security and Cloud Computing Conference*, Jul. 2021.
5. [5] A. Patel and V. Sharma, "Evidence management using smart contracts," in *Proceedings of the International Conference on Blockchain and Internet of Things*, Oct. 2021.
6. [6] R. Singh and P. Kumar, "Chain of custody management using blockchain," *International Journal of Advanced Research in Engineering and Technology*, Apr. 2020.
7. [7] J. Lee and S. Kim, "SHA-256 based tamper-proof storage," *Journal of Information Security*, vol. 12, no. 3, pp. 210–215, Sep. 2020.
8. [8] R. Gupta, S. Mehta, and A. Patel, "Blockchain-based digital evidence storage system," *International Journal of Computer Applications*, Dec. 2019.
9. [9] J. Benet, "IPFS: InterPlanetary File System," Protocol Labs, May 2014.
10. [10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Oct. 2008.

Future scope:

- **Integration with Real Blockchain Networks:** The system can be connected to platforms like Ethereum or Hyperledger to make it more secure fully decentralized.
- **Cloud-Based Deployment:** Hosting the system on cloud platforms like AWS or Azure can improve accessibility, storage, and data management.
- **Mobile Application Development:** A mobile app can allow users to upload and verify evidence directly from the field easily.
- **Enhanced Security Features:** Adding features like multi-factor authentication and encryption can further protect the system.
- **AI-Based Evidence Analysis:** Artificial intelligence can help in automatically analyzing and organizing digital evidence.
- **Scalability Improvements:** The system can be improved to handle large amounts of data efficiently for real-world use.