International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

BLOCK-CHAIN BASED CRIME EVIDENCE SYSTEM

GORLI SATYA GANESHWAR
Reg. No. 24Q71F0019
gorlisatyaganeshwar@gmail.com

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY(Autonomous)
Under the guidance of Mr. S. KESAVA RAO MTech (PhD)
kesav546@gmail.com

Abstract*—The integrity and traceability of crime evidence play a vital role in ensuring fair and just legal proceedings. Traditional systems for managing evidence suffer from centralization, vulnerability to tampering, lack of transparency, and inefficient tracking mechanisms. To address these issues, this paper proposes a blockchain-based crime evidence system designed to ensure immutability, transparency, and enhanced security. The system leverages cryptographic hashing, symmetric encryption, and a blockchain structure to maintain an unalterable chain of custody. Features include secure user authentication, geo-location tracking, QR code-based verification, and comprehensive audit logging. Developed using technologies such as Python, Streamlit, SQLite, bcrypt, Fernet, and SHA-256, the system provides a robust platform for digital evidence handling. Functional and security testing confirms the effectiveness of core mechanisms including tamper detection and access control. While the system demonstrates promising capabilities, challenges related to scalability, storage, and legal compliance remain. Future enhancements include integration with enterprise blockchain platforms and adoption of advanced cryptographic protocols.*

Keywords*—Blockchain Technology; Crime Evidence Management; Data Integrity; Chain Of Custody; Digital Forensics.*

I. INTRODUCTION

In the modern criminal justice system, the management of digital evidence plays a pivotal role in ensuring accurate and fair legal outcomes. However, traditional systems used for evidence handling are often centralized, manual, and vulnerable to tampering, unauthorized access, and data loss. These limitations compromise the integrity and traceability of evidence, which are essential for maintaining trust among stakeholders such as law enforcement, forensic experts, and judicial authorities. To mitigate these challenges, this paper presents a blockchain-based crime evidence system that ensures immutability, transparency, and security throughout the lifecycle of digital evidence.

The proposed system utilizes blockchain technology to create a tamper-proof ledger of evidence records. Each entry is cryptographically secured and linked to the previous one, forming an immutable chain. Additional features include secure user authentication, role-based access control, file encryption,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

geo-location tracking, and QR code-based verification. These components work together to provide a comprehensive solution for managing digital evidence while addressing the shortcomings of conventional systems.

II. LITERATURE SURVEY

Several researchers have explored the application of blockchain technology in various domains, including cybersecurity and digital forensics. Nakamoto introduced the concept of a decentralized and immutable ledger through Bitcoin, laying the foundation for blockchain applications beyond cryptocurrency [1]. Zyskind et al. proposed a privacy-preserving data management model using blockchain and cryptography, although scalability remained a challenge [2]. Kshetri highlighted the potential of blockchain in enhancing data security and transparency, though practical implementations were limited [3].

In the context of digital evidence, Lone and Mir developed a system using blockchain and hashing to secure the chain of custody, but faced storage limitations [4]. Sharma et al. integrated smart contracts to automate access control and validation, although complexity in implementation was noted [5]. Kumar et al. combined encryption with blockchain to enhance confidentiality and integrity, albeit at a high computational cost [6]. Singh et al. incorporated geo-tagging to improve traceability and auditing, yet acknowledged legal acceptance issues [7].

TABLE I. LITERATURE SURVEY TABLE

S.No	Author(s) / Year	Title / Approach	Technology Used	Key Contribution	Limitations
1	Nakamoto (2008)	Bitcoin Blockchain	Blockchain	Introduced decentralized and immutable ledger	Not specific to evidence systems
2	Zyskind et al. (2015)	Decentralized Data Management	Blockchain + Cryptography	Ensured privacy-preserving data storage	Scalability issues
3	Kshetri (2017)	Blockchain in Cybersecurity	Blockchain	Improved data security and transparency	Limited real-world implementation
4	Lone & Mir (2019)	Digital Evidence Management	Blockchain + Hashing	Secure chain of custody	Storage challenges
5	Sharma et al.	Forensic Evidence	Blockchain +	Automated access control	Complexity in

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

	(2020)	System	Smart Contracts	and validation	implementation
6	Kumar et al. (2021)	Secure Evidence Storage	Encryption + Blockchain	Enhanced confidentiality and integrity	High computational cost
7	Singh et al. (2022)	Blockchain-based Forensics	Blockchain + Geo-tagging	Improved traceability and auditing	Legal acceptance issues

III. EXISTING SYSTEM AND PROPOSED SYSTEM

A. Existing System

Current systems for managing crime evidence are predominantly centralized and manual. Evidence records are typically stored in centralized databases, which are vulnerable to tampering and unauthorized access. There is often a lack of proper tracking mechanisms, resulting in incomplete chain of custody records. Additionally, these systems do not offer real-time verification of evidence authenticity, increasing the risk of undetected tampering. Data loss due to system failures or cyberattacks is another concern, along with limited transparency that undermines stakeholder trust.

B. Proposed System

The proposed system addresses the limitations of existing systems by implementing a blockchain-based architecture. Key features include immutability, where evidence records cannot be altered once stored; transparency, enabling verification of all transactions; and enhanced security through encryption and hashing techniques. The system also maintains a complete chain of custody by logging every action, and reduces dependency on a single authority through conceptual decentralization. Additional functionalities include secure login, file encryption, blockchain record storage, QR code verification, geo-location tracking, and audit logging.

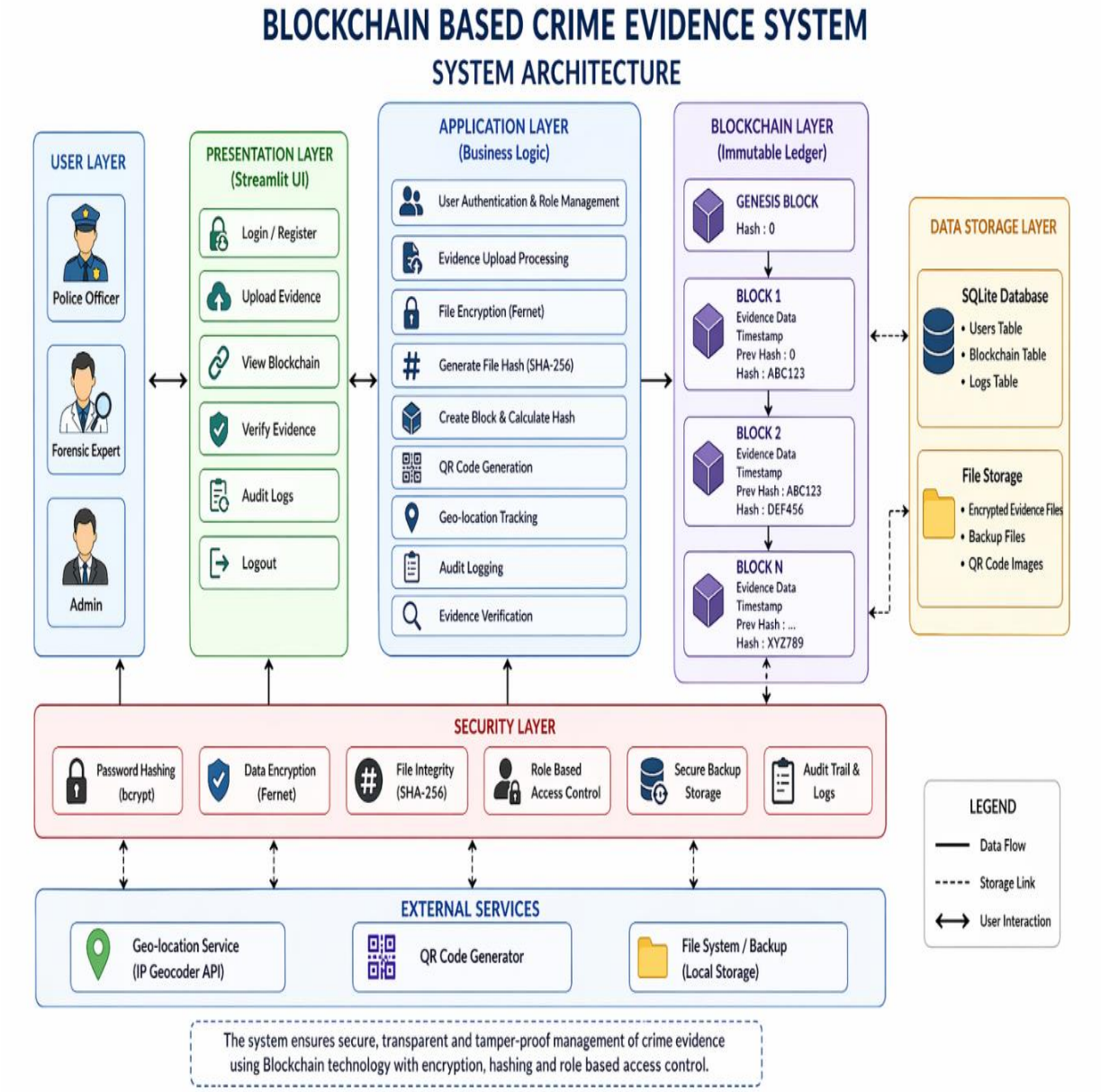
IV. SYSTEM DESIGN AND ARCHITECTURE

The Blockchain-Based Crime Evidence System is structured using a layered architecture that integrates user interaction, application logic, security mechanisms, and data storage. This design ensures secure, transparent, and tamper-proof handling of digital evidence.

- Presentation Layer (User Interface): Built using Streamlit UI, providing interfaces for registration, login, evidence upload, blockchain viewing, evidence verification, and audit logs.
- Application Layer (Business Logic): Manages user authentication, role-based access, evidence upload processing, encryption/decryption, hash generation, blockchain creation, QR code generation, and activity logging.
- Security Layer: Implements bcrypt for password hashing, Fernet for symmetric encryption, SHA-256 for file integrity, secure backups, and role-based access control.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Blockchain Layer: Maintains a chain of evidence records, with each block containing evidence details, timestamp, user info, geo-location, previous hash, and current hash.
- Data Storage Layer: Uses SQLite for storing user data, blockchain records, and audit logs; stores encrypted evidence files, backups, and QR codes separately.
- External Services Layer: Integrates geo-location APIs, QR code generators, and file system storage.



V. SYSTEM IMPLEMENTATION

The system is implemented using a combination of programming languages and tools. Core technologies include Python for backend logic, Streamlit for the user interface, and SQLite for database

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

management. Security features are realized through bcrypt for password hashing, Fernet for file encryption, and SHA-256 for generating cryptographic hashes. QR codes are generated for evidence verification, and geolocation data is captured using the geocoder library. Additional libraries such as NumPy, pandas, OpenCV, Pillow, scikit-image, TensorFlow CPU, LIME, and matplotlib support various functionalities including image processing and machine learning interpretability.

Version-specific dependencies used in the implementation include streamlit==1.32.0, pandas==2.2.1, NumPy==1.26.4, opencv-python-headless==4.9.0.80, pillow==10.2.0, scikit-image==0.22.0, tensorflow-cpu==2.15.0, lime==0.2.0.1, and matplotlib==3.8.3.

VI. RESULTS AND DISCUSSION

The system underwent comprehensive testing to validate its functionality, security, and performance. Both functional and non-functional testing methodologies were employed, including black-box and white-box testing. Unit testing confirmed the correct behavior of individual modules such as user authentication, file encryption, hash generation, and blockchain block creation. Integration testing verified interactions between modules, while system testing ensured end-to-end functionality.

Security testing validated the effectiveness of password hashing and encryption mechanisms, confirmed prevention of unauthorized access, and demonstrated successful detection of file tampering through hash comparison. Performance testing indicated stable and responsive system behavior during file uploads and verifications. User acceptance testing confirmed that the interface was intuitive and met user expectations.

TABLE II. BLACK BOX TESTING TABLE

Feature	Input (Test Case)	Expected Output
Registration	Valid email and password.	Account created; redirected to Login.
Evidence Upload	Uploading a .jpg or .pdf file.	System displays "Upload Successful" and shows a Hash.
QR Generation	Successfully uploaded file.	A scannable QR code appears on the screen.
Validity Check	Uploading a modified version of the original file.	System displays "Invalid/Tampered Evidence" error.
Login Security	Entering an incorrect password 5 times.	Accounts are temporarily locked.

TABLE III. TEST CASES

Test Case ID	Test Scenario	Input	Expected Output	Result

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

TC01	User Registration	Valid username & password	User registered successfully	Pass
TC02	User Login	Correct credentials	Login successful	Pass
TC03	Invalid Login	Wrong password	Error message displayed	Pass
TC04	Upload Evidence	Valid file	File encrypted & stored	Pass

VII. CHALLENGES AND LIMITATIONS

Despite its advantages, the proposed system faces several challenges. Internet connectivity is required for features such as geo-location tracking. The blockchain implementation is currently simulated rather than fully decentralized. Storage constraints may affect handling of large multimedia files. Legal and regulatory acceptance varies across jurisdictions. Scalability and privacy concerns, as identified in prior research, also pose ongoing challenges.

VIII. CONCLUSION AND FUTURE SCOPE

This paper presented a blockchain-based crime evidence system aimed at overcoming the limitations of traditional evidence management systems. By leveraging cryptographic techniques and blockchain architecture, the system ensures data integrity, traceability, and security. Testing results confirm the effectiveness of core functionalities such as tamper detection and access control. However, challenges related to scalability, storage, and legal compliance persist.

Future enhancements include transitioning to a fully decentralized blockchain network such as Ethereum or Hyperledger for improved consensus and validation. Integration with distributed storage solutions like IPFS could alleviate storage burdens. Implementation of smart contracts may automate chain of custody procedures. Incorporation of AI-powered forensic analysis, biometric authentication, and zero-knowledge proofs could further enhance security and privacy. Additionally, mobile applications and IoT integration could facilitate real-time evidence capture and upload. Legal interoperability and compliance with national and international standards will also be critical for widespread adoption.

Representative figures from the system are listed below:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

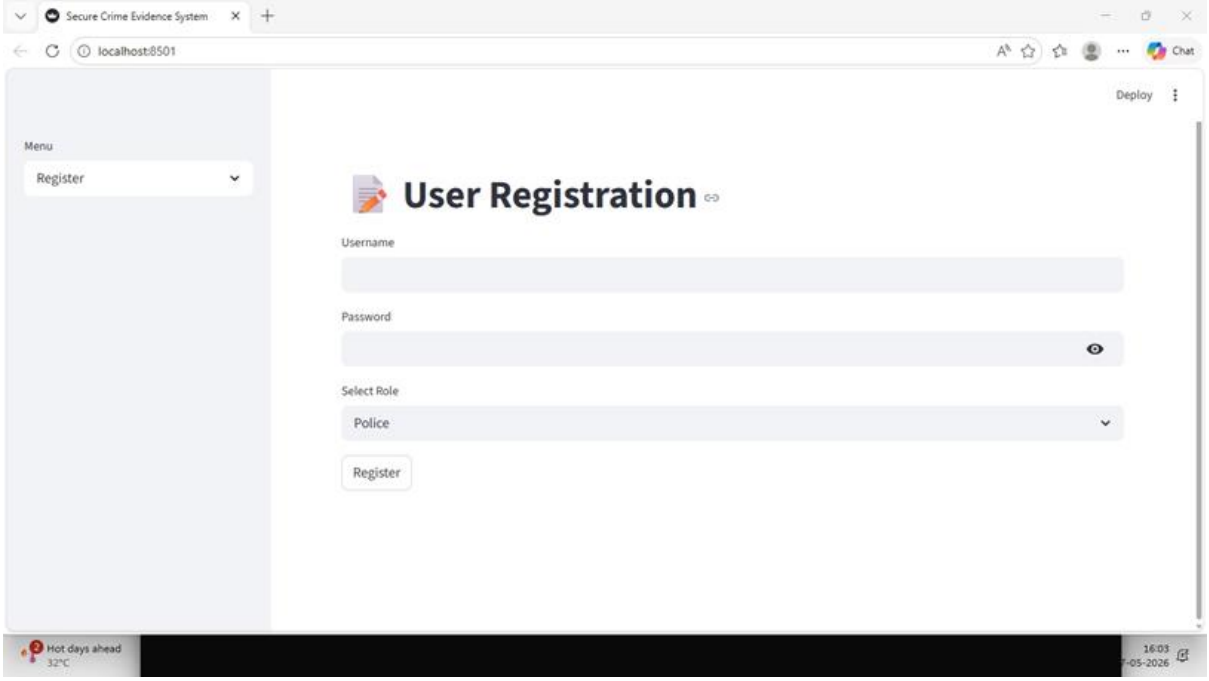


Fig. 1. Registration Page

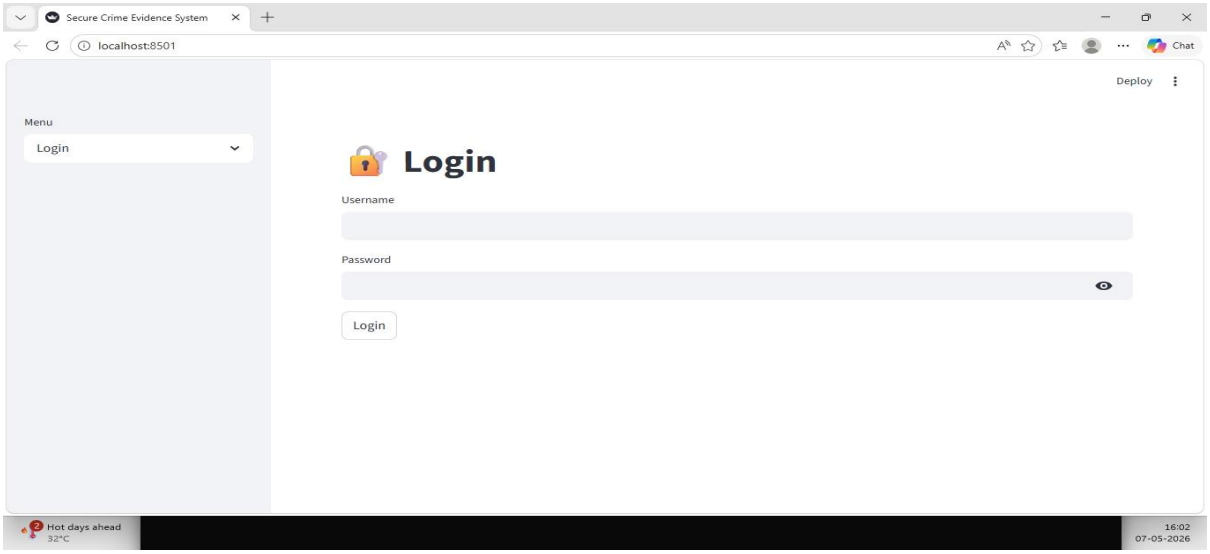


Fig. 2. Login Page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

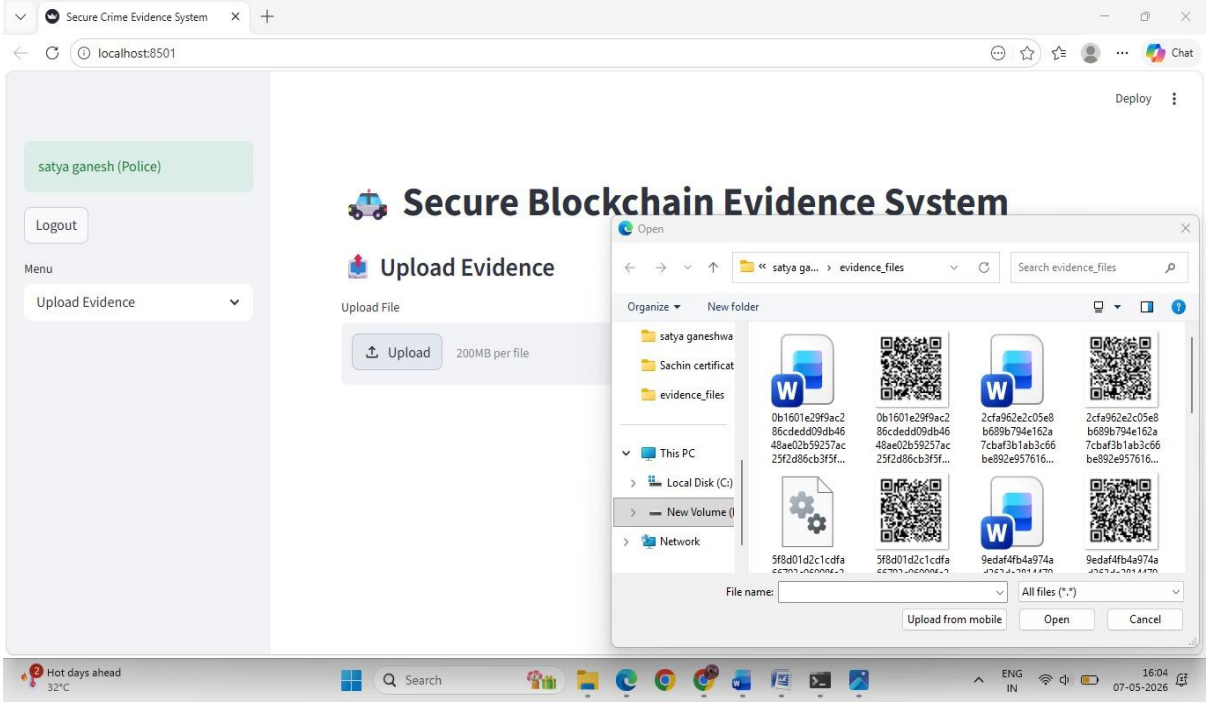


Fig. 3. Upload Evidence file

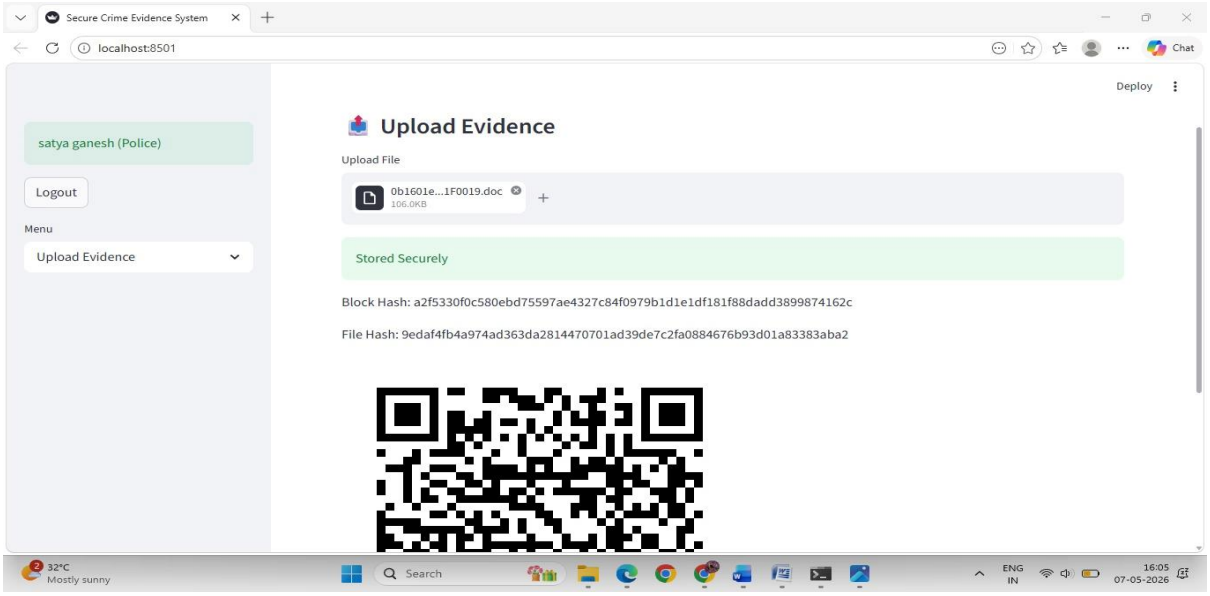


Fig. 4. QR code Generator for files

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

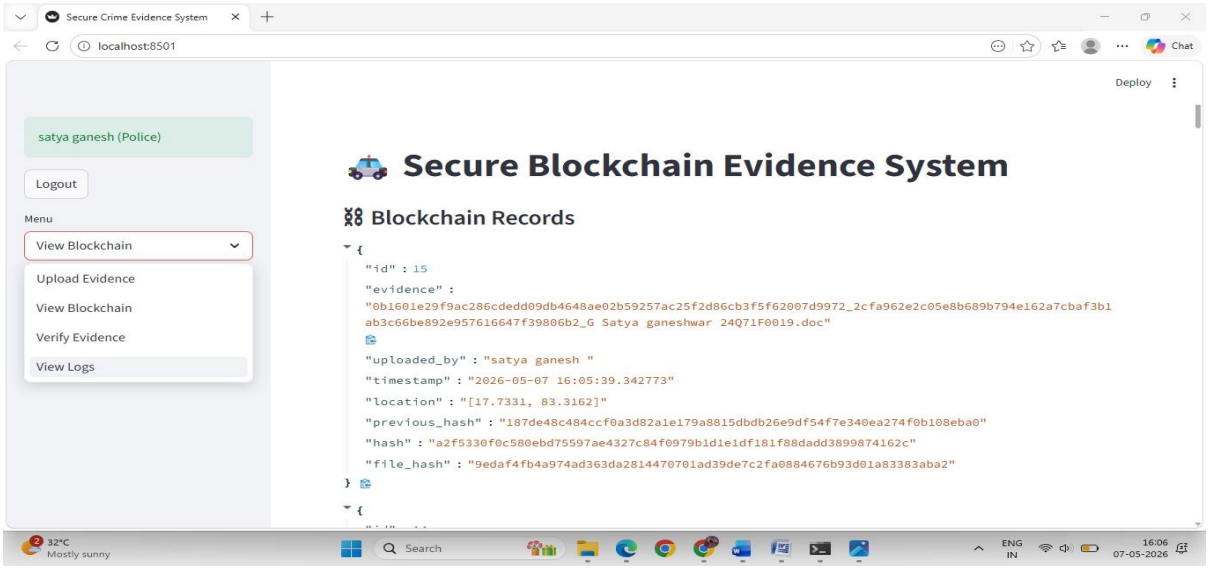


Fig. 5. Hash code Generator

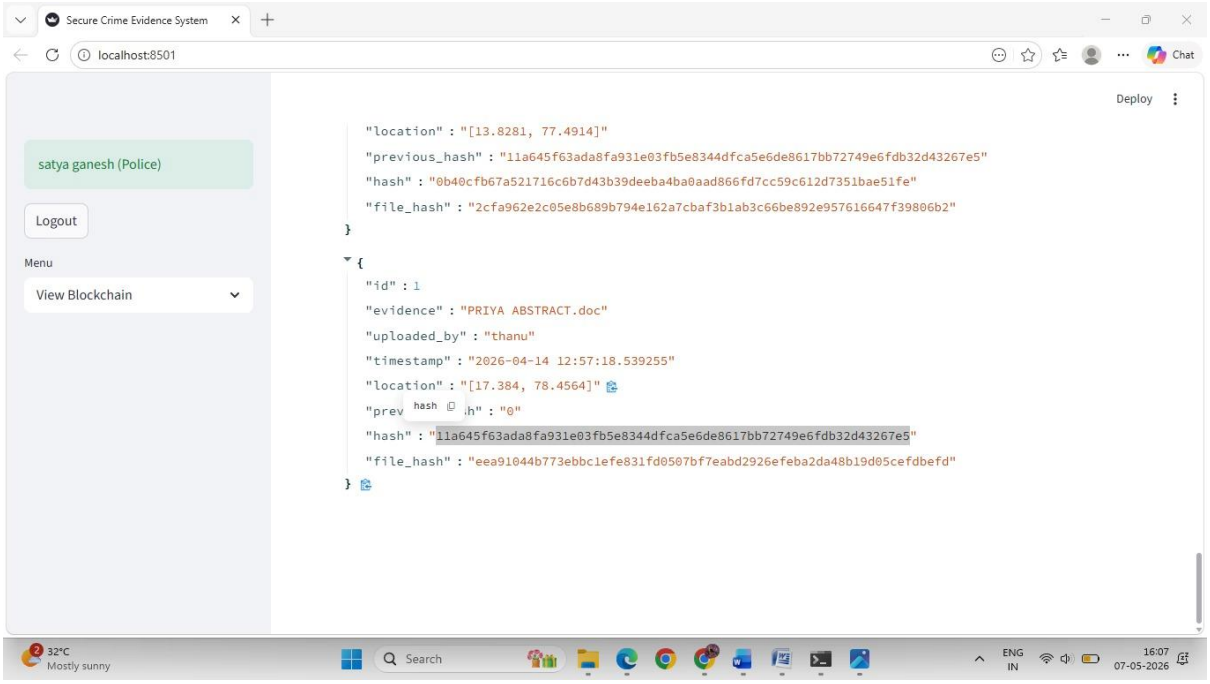


Fig. 6. Access Hash code

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

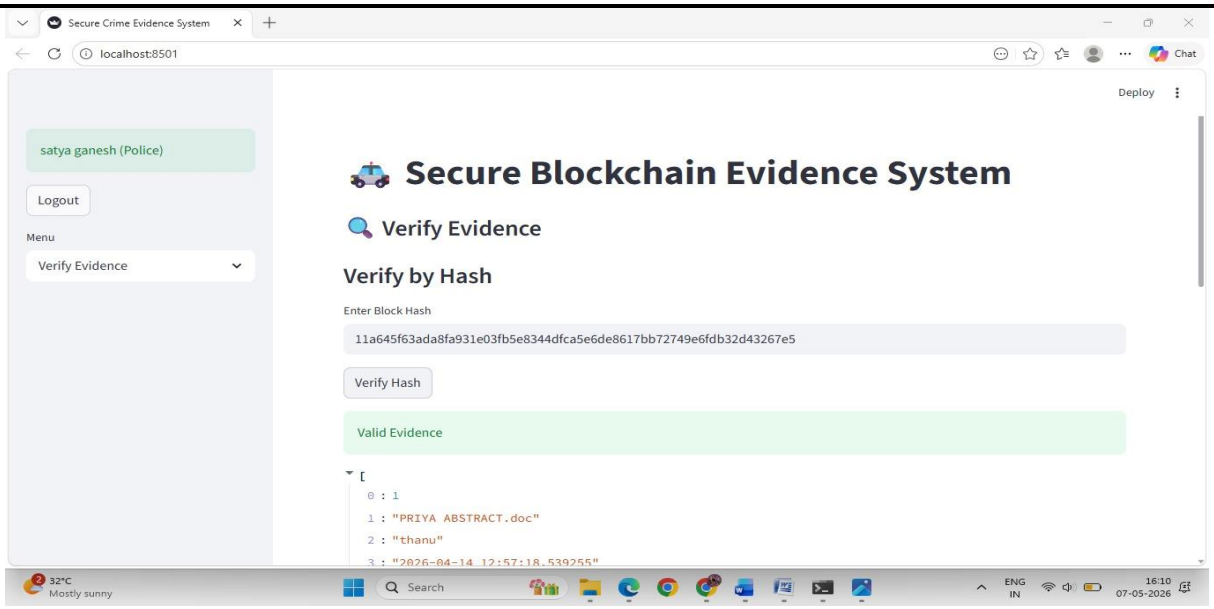


Fig. 7. Validation and metadata

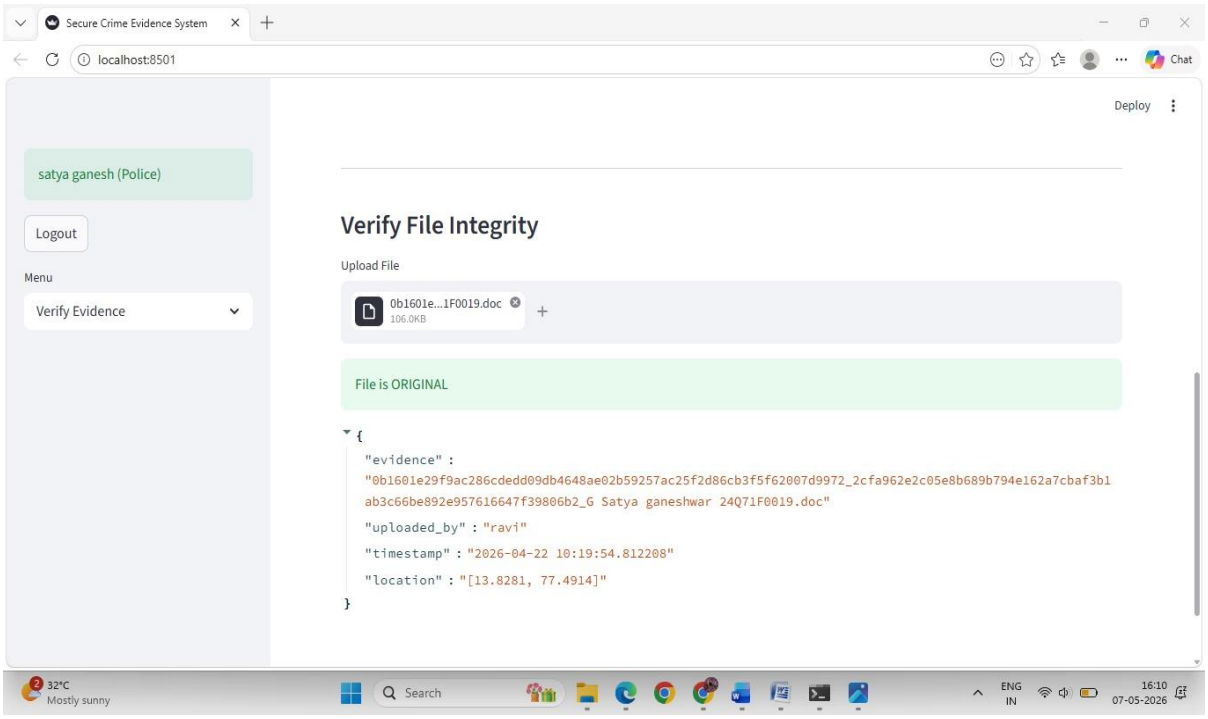


Fig. 8. Check Evidence Validation

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

REFERENCES

[1] Jyoti, A., & Chauhan, R. K. (2022). A blockchain and smart contract-based data provenance collection and storing in cloud environment. Wireless Networks, 28(4), 1541-1562. https://doi.org/10.1007/s11276-022-02924-y

[2] Chauhan, A. (2025). Evi Chain: A Blockchain based Evidence Management System. JUIT Research Repository.

[3] Kuznetsov, O., Serani, P., Romeo, L., Frontino, E., & Mancini, A. (2024). On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. IEEE Access, 12, 3881-3897. https://doi.org/10.1109/access.2023.3349019

[4] Saidu, Y., Shuhada, S. M., Aliyu, D. A., Abdul Aziz, I., & Adamu, S. (2025). Convergence of Blockchain, IoT, and AI for Enhanced Traceability Systems: A Comprehensive Review. IEEE Access, 13, 16838-16865. https://doi.org/10.1109/access.2025.3528035

[5] Haji, I. A. (2026). Blockchain based chain of custody and digital evidence legality in post conflict prosecutions. Frontiers in Blockchain, 9, Article 1801364.

[6] Igonor, O. S., Amin, M. B., & Garg, S. (2025). The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review. Blockchains, 3(1), 5. https://doi.org/10.3390/blockchains3010005

[7] Han, P. (2025). AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. PubMed Central.

[8] Ramaz amba, P. T. (2025). Blockchain Forensics and Regulatory Technology for Crypto Tax Compliance: A State-of-the-Art Review and Emerging Directions. MDPI Applied Sciences.