NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

Revolutionizing Evidence Handling: Mobile Interface Meets Secure Blockchain Technology

A Y V Krishna
School of Cyber Security and Digital Forensics
NFSU,
Gandhinagar, India

Dr. Ravirajsinh S. Vaghela
School of Cyber Security and Digital Forensics,
NFSU,
Gandhinagar, India

Dr. Naveen Kumar Chaudhary
School of Cyber Security and Digital Forensics,
NFSU,
Gandhinagar, India

***Abstract*— Mobile applications are revolutionizing evidence tracking and management. They streamline processes through real-time data capture, automated workflows, and remote access. Secure storage with mobile apps and blockchain integration guarantees evidence of authenticity and integrity. Additional benefits include reduced costs, improved data quality, and enhanced user experience. However, challenges like blockchain scalability, privacy concerns, and standardization require careful consideration when implementing these technologies. The paper emphasizes the benefits of mobile apps while acknowledging the complexities of blockchain adoption in evidence management. The paper proposed an idea to store and implementation.**

Keywords—Blockchain; Mobile Application; Evidence management

I. INTRODUCTION

The landscape of evidence handling is rapidly evolving, and mobile applications are emerging as powerful tools for streamlining processes, enhancing security, and improving efficiency. Here's why mobile apps are becoming increasingly important in evidence tracking and management. Real-time data capture: Photos, videos, and audio recordings of evidence can be captured directly at the scene, eliminating manual paperwork and reducing time delays. Automated workflows: Mobile apps can automate routine tasks like chain of custody updates, evidence tagging, and data entry, saving valuable time and resources. Remote access: Authorized personnel can access and update evidence information from anywhere, facilitating collaboration and improving responsiveness. Tamper-proof evidence: Data stored on secure mobile apps with blockchain integration guarantees the authenticity and integrity of evidence through tamper-proof timestamps and audit trails. Restricted access: Role-based access controls within the app ensure only authorized users can view and manage specific evidence items, minimizing the risk of unauthorized access. Offline functionality: Evidence data can be captured and stored offline in case of network connectivity issues, ensuring uninterrupted evidence collection. Real-time updates: Stakeholders can access real-time updates on the chain of custody, enhancing transparency and accountability throughout the evidence lifecycle. Secure communication: Secure messaging features within the app facilitate communication between investigators, prosecutors, and other authorized parties. Shared situational awareness: Real-time location tracking of evidence and personnel can improve situational awareness for investigators and first responders. Another benefit of implementing reduced costs: Streamlined workflows and improved efficiency can lead to significant cost savings compared to traditional paper-based systems. Improved data quality: Mobile apps can capture richer data in various formats, leading to more comprehensive and accurate evidence records. Enhanced user experience: Intuitive and user-friendly mobile apps improve the experience for evidence-collection personnel and authorized users.

Blockchain-based evidence management needs to be considered, depending on the sensitivity of the information and trust level between participants, public or private blockchain can be used. Public blockchain offer maximum transparency, while private blockchain provides more control and access restrictions. Proof-of-Work (PoW) is the most common consensus mechanism in public blockchain, but alternative mechanisms like Proof-of-Stake (PoS) are gaining traction due to their energy

efficiency. Private Blockchain can employ various consensus mechanisms tailored to specific needs [1] [2].

Consensus mechanism	Network Type	Trust-Model	Reference
POW (proof of work)	Pu.	UT	[1],[2],[3],[4]
POS (proof of stake)	Pu.	UT	[1],[2],[3],[4]
DPoS (Delegated Proof of Stake)	Pu.	UT	[1],[2],[3],[4]
PBFT (Practical Byzantine Fault Tolerance)	Pr.	ST	[1],[2],[5],[6]
PoA (Proof-of-Authority)	Pr.	T	[1],[2],[6]
PoC (proof-of-contribution)	Pr.	ST	[1],[2],[7],[8]
PoET (Proof of elapsed time)	Pr./Con.	ST	[1],[2],[9]
RAFT (Reliable, Replicated, Redundant, And Fault-Tolerant)	Pr./Con.	ST	[1],[2],[10]

Interoperability and Integration: Integrating blockchain-based evidence management systems with existing legal and law enforcement systems requires careful consideration of data formats, APIs, and standards to ensure seamless communication and data exchange.

Technical considerations should be taken care such as 1) Scalability: Can large evidence datasets be secured on-chain? 2) Sharding and off-chain storage offer solutions. Privacy: Balancing transparency with privacy is key. Sensitive data might need anonymization or encryption. 3) Security: Robust protocols like secure key management are crucial to prevent unauthorized access and attacks. Standardization efforts are ongoing.

II. Current Practices of Case and Evidence Handling in Indian Police Departments:

A. *Strength*

Established Procedures: The Criminal Procedure Code (CrPC) and other legal guidelines provide a framework for investigation and evidence handling. Focus on Physical Evidence: Traditional forms of evidence like fingerprints, handwriting samples, and physical objects are collected and documented. Forensic Units: Some states have dedicated forensic science labs for analyzing evidence, though nationwide coverage is uneven.

B. *Weakness*

Limited Resources: Manpower and technological resources are often strained, hindering thorough investigations and efficient evidence management. Paper-based System: Evidence documentation largely relies on paper records, susceptible to loss, damage, and manipulation. Chain of Custody Issues: Maintaining an unbroken chain of custody for evidence can be challenging due to manual processes and lack of real-time tracking. Delayed Investigations: Long investigation times can weaken evidence integrity and hamper justice delivery.

C. *Recent Development*

National Crime Records Bureau (NCRB): NCRB aims to improve standardization and data collection through initiatives like the Crime and Criminal Tracking Network System (CCTNS). Digitalization Initiatives: Some states are piloting projects for digital evidence management and e-FIRs.
Focus on Training: Training programs for police officers on modern investigative techniques and evidence handling are being emphasized.

D. *Challenges Remain*

Funding Shortages: Digital solutions and capacity-building implementation require consistent funding and infrastructure development.
Cybercrime Expertise: Equipping police forces to handle cybercrime evidence effectively is crucial in the digital age.
Public Trust: Building public trust in police procedures and evidence-handling practices is essential for a stronger justice system.

III. Related Work

Block-DEF, a loosely coupled blockchain-based system in [11], tackles file manipulation through optimized PBFT, scalable structure, and multi-signature systems, demonstrably meeting digital evidence security standards [11]. "Digital Witness," a mobile security architecture, was thoroughly analyzed in the article [12]. Study proposes a secure, Blockchain-based framework with Rijndael & SHA encryption for forensic/medical data, emphasizing improved evidence quality and tamper-proof transfers for successful investigations in law enforcement [13]. Paper [14] proposes a secure, blockchain-integrated SDN-IoT forensic architecture, improving efficiency and security in managing diverse traffic types compared to prior work [14]. Article [15] reviews Digital Forensics (DF) methods, tools, and trends, finding EnCase excels in data recovery. It considers human factors and outlines Digital Forensic Readiness (DFR) parameters. The research helps choose tools and models for better investigations. Future AI integration holds promise for further progress [15]. Paper [16] proposes a blockchain-based system for secure custody and sharing of digital files in forensic medicine. Potential

applications include securely storing consent forms, healthcare directives, and medical images. Future improvements could involve file size variations for access control and automatic file encryption [16]. Marking the final step in digital forensics, the reporting stage translates meticulous findings into a detailed NIST-compliant report [17]. Secure evidence management is vital in forensics, ensuring justice and preventing case dismissal. Traditional methods risk tampering, so a digital system is crucial.

Blockchain, a secure, transparent ledger, offers potential for evidence management. This study explores adapting Hyperledger Fabric, an enterprise blockchain framework, to create a digital forensics system [18]. This paper proposes a consortium blockchain system for standardized and secure electronic evidence generation, collection, and verification, bolstering evidence credibility and legal force[19]. LEChain uniquely provides anonymous witness authentication, fine-grained access control for evidence, secure jury voting, and covers the entire digital forensics evidence lifecycle within a blockchain framework, addressing key privacy concerns [20].

IV. PROPOSED SOLUTION

The primary objective of this application is to improve the integrity and trust of evidence gathered during investigation by ensuring transparency in the chain of custody and storing the evidence in an immutable (tamper-proof) way and providing convenient 24x7 query access of case evidence to all stakeholders. This application plays an important role in securing the evidence from Investigating Officers and Police Station Staff from trying to conceal, falsify or destroy evidence with an intent to manipulate the investigation of a criminal case.

Once the Investigating Officer enters case details in the mobile app, the app invokes an API and a unique case ID will be generated and the blockchain service is invoked. The Investigating Officer then uploads photographs/videos/digital files of a seizure/Crime scene/arrested accused and enters the metadata, seizure/accused name, and description. Once a file is uploaded from the mobile app onto the server, it will be stored in a designated location on the server along with metadata. The content of the file is hashed using the hashing algorithm. This hash acts like a fingerprint of the file content and the hash and metadata of the file are saved onto blockchain.

During future verification, the hash is computed from the content of the file located on the server and this hash is then compared with the respective hash already stored in the blockchain. When both hashes match, the verification process is marked as successful. Access can be given to courts and defense during trial. This Application was developed as a Proof of Concept and can be implemented by state police/investigating agencies by scaling up the same.

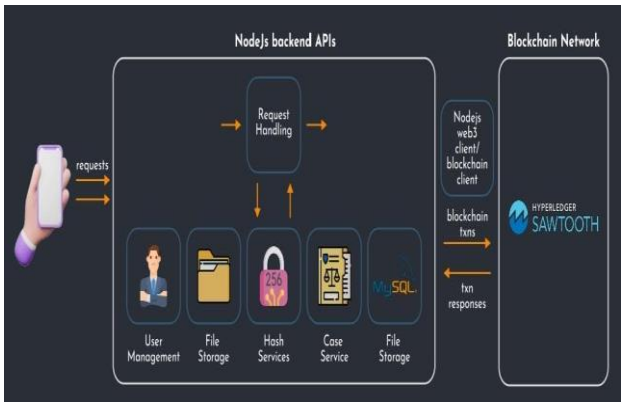

Figure 1 Background Detail of Storage Management of Evidence

Figure 1 gives details about how mobile application will take the help of hyperledger sawtooth technology to store the hash value of evidence metadata. Other details like which officer right now inserting the evidence with the user management module and storing images of evidence with different views and directions with metadata in the file storage system and all data will be secure. This proposed system also works on the case system service and inserts details about the case which uses mysql database to store information and at last hash stored into blockchain.

Technical considerations are taken care of when the proposed solutions are as follows:

Scalability: Can large evidence datasets be secured on-chain? Sharding and off-chain storage offer potential solutions.

Privacy: Balancing openness with data privacy is key. Sensitive data might need anonymization or encryption on the blockchain.

Security: Robust protocols like secure key management are crucial to prevent unauthorized access and attacks on evidence data.

Standardization: Lack of standardized protocols creates adoption hurdles. Efforts are ongoing to develop industry-wide standards and best practices.

Chain of Custody

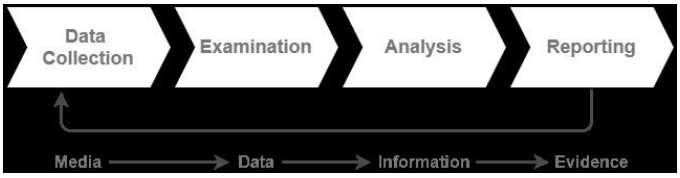

Figure 2 Chain of custody steps

While the traditional chain of custody protocols serve a purpose, they are increasingly cumbersome and susceptible to human error. Blockchain technology, with its inherent

immutability and distributed ledger system, offers a novel and technically robust solution.

Imagine a system where every interaction with evidence, from collection to analysis, is cryptographically hashed and linked onto a tamper-proof blockchain. This creates an auditable, transparent record of every handoff, eliminating the need for paper trails and manual entries. Smart contracts can automate chain of custody updates, triggering notifications and access restrictions based on predefined rules. Further, decentralized storage solutions built on blockchains can ensure data redundancy and prevent unauthorized modifications.
In this application, one officer is assigned to collect the evidence put it as seizure, and take photos in a blockchain-backed mobile application as shown in Figure 3.

Figure 3 Seizure Data

After collecting all the evidence with the case ID and collector officer detail and authority given by also giving auto seizure ID with a unique ID where the officer needs to give detail about the evidence who entered this detail and what is role and type of seizure data whether its images audio or video.
Next step of Seizure is tracking the evidence and its place latitude and longitude and also verifying all the metadata about the evidence with blockchain-backed and stored hash value. Figure 4 helps to track the evidence with its metadata information of the police station and its geographical location.

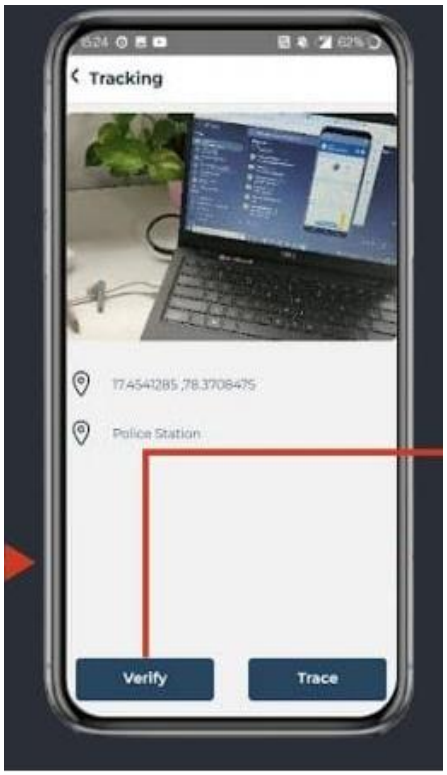

Figure 4 Tracking evidence with its latitude & longitude

After completing tracking one verifies the Hash value of evidence in digital format via Hyper ledger sawtooth.

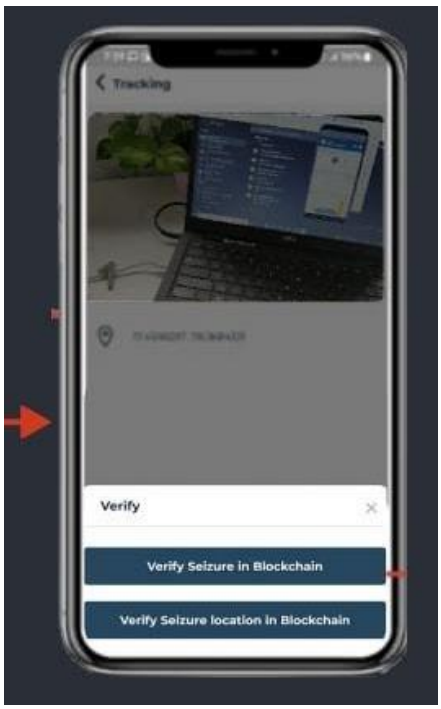

Figure 5 Tracking and Verify Evidence

V. CONCULSION

Scalability issues arise when dealing with large volumes of evidence data. Balancing transparency with data privacy necessitates careful encryption and access control mechanisms. Regulatory frameworks and standardized protocols for evidence management on blockchains are still evolving. Despite these challenges, the potential of blockchain to revolutionize the chain of custody is undeniable. By leveraging its technical strengths and addressing existing limitations, we can pave the way for a secure, transparent, and efficient system for handling evidence in the digital era. This proposed solution makes faith and trust in police investigation systems and evidence management.

REFERENCES

[1] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). Ieee, 2017.

[2] Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. "A survey of blockchain consensus algorithms performance evaluation criteria." Expert Systems with Applications 154 (2020): 113385

[3] Baliga, Arati. "Understanding blockchain consensus models." Persistent 4.1 (2017): 14.

[4] Bouraga, Sarah. "A taxonomy of blockchain consensus protocols: A survey and classification framework." Expert Systems with Applications 168 (2021): 114384.

[5] Altarawneh, Amani, and Anthony Skjellum. "The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms." 2020 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2020

[6] De Angelis, Stefano, et al. "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain." CEUR workshop proceedings. Vol. 2058. CEUR-WS, 2018.

[7] Song, Hongyu, et al. "Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection." Information processing & management 58.3 (2021): 102507.

[8] Tian, Zhihong & Li, Mohan & Qiu, Meikang & Sun, Yanbin & Su, Shen. (2019). Block-DEF: A Secure Digital Evidence Framework using Blockchain. Information Sciences. 491. 10.1016/j.ins.2019.04.011

[9] Chen, Lin, et al. "On security analysis of proof-of-elapsed-time (poet)." Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19. Springer International Publishing, 2017.

[10] Yao, Wei, et al. "A survey on consortium blockchain consensus mechanisms." arXiv preprint arXiv:2102.12058 (2021).

[11] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," IEEE Netw., vol. 30, no. 6, pp. 34–41, Nov. 2016

[12] Shrunga, H & M, Ashwini & U, Deepthi & R, Spandana & R, Rakesh. (2022). A Survey on Blockchain Based Digital Forensics Framework. International Journal for Research in Applied Science and Engineering Technology. 10. 2542-2549. 10.22214/ijraset.2022.41841

[13] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," IEEE Access, vol. 7, pp. 99573–99588, 2019.

[14] Dubey, Himanshu, Shobha Bhatt, and Lokesh Negi. "Digital Forensics Techniques and Trends: A Review." The International Arab Journal of Information Technology (IAJIT) 20.4 (2023): 644-654.

[15] M. Lusetti, L. Salsi, and A. Dallatana, "A blockchain based solution for the custody of digital files in forensic medicine," Forensic Sci. Int., Digit. Invest., vol. 35, Dec. 2020, Art. no. 301017.

[16] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, “Blockchain on security and forensics management in edge computing for iot: A comprehensive survey,” IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1159–1175, 2021.

[17] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Sp 800-86. guide to integrating forensic techniques into incident response,” 2006.

[18] Sathyaprakasan, Revathy, et al. "An implementation of blockchain technology in forensic evidence management." 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). IEEE, 2021.

[19] Chen, Shijie, et al. "Study and implementation on the application of blockchain in electronic evidence generation." Forensic Science International: Digital Investigation 35 (2020): 301001.

[20] Li, Meng, et al. "LEChain: A blockchain-based lawful evidence management scheme for digital forensics." Future Generation Computer Systems 115 (2021): 406-420.