An Implementation of Forensic Evidence Management under AWS-S3 Service

Dr. Archana B[1], Adithya Baragi S[2], Anusha K N[3], Jeevan Basri B S[4], Karthik E M[5]

[1]Associate Professor, Department of Computer Science and Engineering
[2, 3 ,4,5]Student, Department of Computer Science and Engineering
Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

ABSTRACT

In the realm of forensic science, effective evidence management is paramount to ensuring the integrity and admissibility of evidence collected from crime scenes. The Chain of Custody (CoC) process plays a pivotal role in safeguarding this integrity by tracking and documenting the custody of evidence throughout its lifecycle. Blockchain technology offers a compelling solution to enhance CoC processes by providing a decentralized, immutable, and transparent ledger system. The digitalization of forensic evidence management through blockchain presents a contemporary and environmentally sustainable approach. Blockchain operates as a distributed ledger where transactions are securely recorded in a chronological order within blocks, accessible to all participants in the network. This study endeavours to devise a comprehensive framework and algorithm to integrate blockchain into forensic evidence management, focusing on establishing and maintaining the Chain of Custody seamlessly. The proposed solution aims to leverage blockchain's inherent features of transparency, immutability, and cryptographic security to fortify the evidentiary trail, thereby ensuring the credibility and admissibility of digital forensic evidence in legal proceedings.

Keywords : *- Forensic Evidence Management, Blockchain, Chain of Custody, AWS-S3, Security*

1. INTRODUCTION

Evidence management is critical in the field of forensic science. Managing evidence effectively is crucial within the realm of forensic science. A primary concern in forensic investigations lies in the meticulous handling and documentation of evidence, from its initial extraction through to its presentation in court. Maintaining the integrity of evidence is paramount throughout this process. Chain of Custody (CoC) involves documenting the handling of evidence in a chronological sequence during the investigation, ensuring its acceptance as valid in court proceedings. Specific criteria must be adhered to during the CoC procedure: preventing corruption or alteration of evidence to maintain reliability, tracing the flow of evidence custody within the jurisdiction during investigation, ensuring relevance and reliability of presented evidence for the crime in question, enabling every entity that interacts with the evidence to verify the process, and preventing unauthorized access to avoid tampering.

Digitalizing forensic evidence management not only conserves space but also promotes environmental friendliness and cost-efficiency. The authenticity and legitimacy of CoC are crucial for rendering evidence admissible in court, which can be upheld using Blockchain technology. Blockchain allows for secure storage and access of system details within a single network, streamlining processes and reducing the time spent reviewing physical documents.

2. RELATED WORK

2.1 Chain of Custody (CoC)

Evidence forms the cornerstone of any criminal investigation, serving as the primary means to establish guilt or innocence. Without robust evidence, navigating a case becomes exceptionally challenging. Therefore, the careful

handling and processing of evidence are paramount to maintain its integrity and reliability throughout the investigative process.
Chain of Custody (CoC) is the systematic documentation of evidence from the moment it is discovered at the crime scene until it is presented in court during trial. This process is instrumental in ensuring the authenticity and credibility of the evidence. It is the responsibility of investigating officers to oversee that only authorized personnel interact with the evidence and that all documentation is meticulously completed according to standard procedures. Proper handling of evidence entails adhering to established protocols for extraction, processing, and storage. Each step is meticulously documented in an evidence log, which serves as a comprehensive record of the evidence's journey. This documentation is crucial for preventing tampering or alteration of data, thereby preserving the evidential value and integrity.

2.2 Blockchain Technology

Blockchain technology is a decentralized and secure way of recording and verifying transactions or data. In the context of forensic evidence management, blockchain can be applied to enhance the Chain of Custody (CoC) process, ensuring the integrity and credibility of evidence. Blockchain technology can significantly contribute to maintaining the authenticity and credibility of evidence by providing an immutable, transparent, and decentralized ledger for the entire CoC process. Blockchain technology ensures that evidence-related information is securely recorded and accessible only to authorized personnel, reducing the risk of tampering, and enhancing the overall integrity of the criminal justice system

2.3 AWS-S3 services

Amazon Simple Storage Service (Amazon S3) is a scalable object storage service provided by Amazon Web Services (AWS). In the context of the described content about forensic evidence management, AWS S3 can play a crucial role in securely storing and managing the collected evidence. AWS S3 supports the secure storage of evidence, controlled access, and features like versioning that contribute to maintaining the authenticity and credibility of the evidence throughout the investigative process. Moreover, AWS S3 offers extensive logging and monitoring capabilities, enabling forensic investigators to track access to evidence and monitor for any suspicious activities or unauthorized access attempts. The granular access control features allow administrators to define fine-grained permissions, restricting access to sensitive evidence only to authorized personnel.

2.4 Existing System

Traditional methods of managing forensic evidence predominantly rely on either manual record-keeping or centralized databases. Manual approaches are susceptible to human errors, not to mention the constant risk of tampering or mismanagement. Centralized databases expose vulnerabilities to cyber-attacks, unauthorized access, and data corruption. Regrettably, both methods fall short in providing real-time audit capabilities and a foolproof chain of custody, making it increasingly challenging to ensure the unimpeachable integrity of the evidence. This lingering uncertainly not only poses a threat to the sanctity of court proceedings but also raises the unsettling prospect of potential miscarriages of justice. The deficiency in real-time audit capabilities and a secure chain of custody undermines forensic evidence integrity.

3. REVIEW OF LITERATURE

In reference [1] the author, presents the significant hurdles faced by forensic investigators in the realm of digital and cloud technologies. It identifies key challenges such as cross-border jurisdiction, evidence admissibility, privacy concerns, lack of standardization, complex architectures, dynamic cloud environments, and legal/regulatory issues. The paper emphasizes the necessity for collaboration among stakeholders including forensic investigators, cloud service providers, legal experts, and policymakers to address these challenges effectively.

Amidst the evolving landscape of digital forensics, researchers continually propose innovative solutions to confront the dynamic challenges of cloud forensics. The study presented in reference [2] discusses the need to analyze cutting-edge methods in cloud forensics, particularly concerning Digital Forensics and Advanced Encryption Algorithms in cybercrimes.

The reference [3], emphasizes the increasing need for cloud forensics due to the prevalence of illegal access to sensitive data stored in cloud environments. It highlights how many cloud users store vast amounts of data without adequate knowledge of data security or the backend infrastructure.

In exploring the intricacies of forensic investigations, the study presented in reference [4], underscores the critical importance of maintaining evidence integrity from collection at the crime scene to presentation in court. Proposing the implementation of Blockchain technology to digitize the chain of custody, the paper aims to ensure enhanced security, authenticity, and integrity of forensic data transactions. The application of Blockchain is envisaged to improve environmental sustainability and bolster security through encryption, accessible remotely by authorized personnel.

In response to the pressing need for enhanced security and transparency in forensic investigations, reference [5] proposes a secure forensic evidence system aimed at optimizing the chain of limited users responsible for forensic investigations. It utilizes the private Ethereum platform to implement blockchain technology, with smart contracts written in Solidity language. By decentralizing the system, it avoids single point failures and enhances security.

New problems are arising every day in the area of digital forensics. Many researchers have proposed various new solutions to test the attacks in real-time might be situations to deal with the issues and challenges of cloud forensics. The study presented in reference [6] delves into the emerging challenges and solutions in the realm of digital forensics, particularly focusing on cloud environments. It highlights the rapid rise in cyber-attacks and the subsequent need for enhanced security measures, emphasizing the significance of cloud forensics in addressing these concerns.

The reference [7] emphasizes the crucial role of knowledge and awareness in ensuring information security and database security. It stresses the importance of security professionals staying updated with the ever-expanding field of cybersecurity to effectively identify and analyze cyber threats.

In light of the escalating complexity and security concerns surrounding cloud networks, reference [8] addresses the need for a framework to conduct forensic investigations in cloud networks due to the inherent security challenges they pose. It also discusses the implementation of a blockchain-based system to enhance the security of existing systems.

In reference [9] the author, presents a solution for improving the security of existing systems through the implementation of a blockchain-based system. This system ensures the safe transfer, recording, and updating of evidence by storing transactions securely on the blockchain, thereby reducing the overhead of maintaining and tracking transactions separately.

In the quest for heightened security against cyber threats and data manipulation, reference [10] discusses the implementation of Blockchain technology for tamper detection in distributed database systems. By storing transaction timestamps on the Blockchain, the paper successfully pinpoints the location of tampering events, enabling the detection of tamper in a distributed database.

4. PROPOSED SYSTEM

In the realm of forensic evidence management, ensuring the integrity, security, and accountability of digital evidence is paramount. Current systems often face challenges related to data tampering, unauthorized access, and centralized vulnerabilities. To address these issues, this project proposes a novel approach by integrating blockchain technology with AWS S3 services.

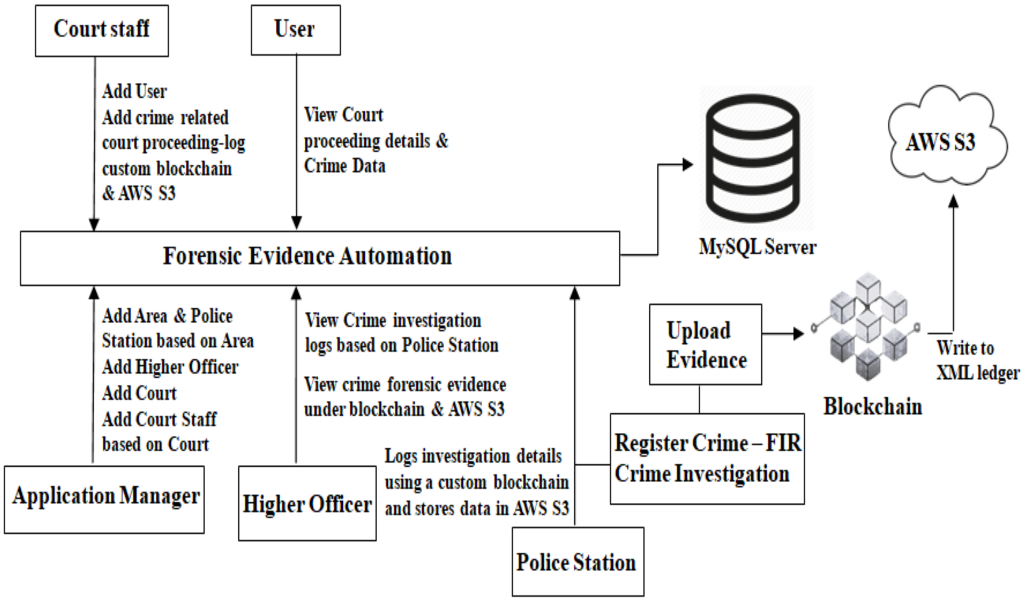

Fig -1 System Architecture

Above **Fig-1** represents the system architecture depicting a Forensic Evidence Automation system related to court proceedings, crime data, and blockchain technology. It includes elements such as court staff, user interactions, crime investigation logs, police stations, and higher officers. The methodology involves a custom blockchain, AWS S3 storage, and MySQL integration. Forensic evidence automation refers to the application of technology and automated systems in the collection, analysis, storage, and management of forensic evidence in legal and investigative processes. Automation in forensic evidence aims to improve efficiency, accuracy, and the overall effectiveness of forensic investigations. Various technologies are employed to streamline and enhance different aspects of the forensic evidence lifecycle. This methodology ensures the secure access and management of critical information at every stage of the criminal justice process, from crime registration to evidence collection and investigation. The involvement of custom Blockchain & AWS S3 storage adds an additional layer of security and reliability, demonstrating a comprehensive framework for effective forensic evidence management.

Furthermore, the flexibility inherent in digital formats allows for easy access by authorized personnel from anywhere in the world, fostering collaboration and enhancing the efficiency of forensic processes. Digitalization also facilitates real-time updates and sharing of information among relevant stakeholders, promoting transparency and expediting investigative procedures. The adoption of digital forensic evidence management systems not only conserves resources but also modernizes investigative practices, aligning them with technological advancements for more effective and streamlined operations.

5. RESULTS & DISCUSSIONS

By implementing a blockchain-based chain of custody, we have established a secure and immutable record of evidence transactions, ensuring the integrity and authenticity of forensic data throughout its lifecycle. This approach has significantly enhanced the transparency and traceability of evidence handling processes, mitigating risks associated with data tampering and unauthorized modifications. One significant modification made in our forensic evidence management system involved implementing restricted access to case details. Unlike the previous system where case information was publicly accessible, we have tailored access permissions so that only authorized users directly involved with the specific crime can view detailed evidence records. This enhancement ensures strict confidentiality and privacy of sensitive information, safeguarding against unauthorized access or misuse by individuals unrelated to the investigation.

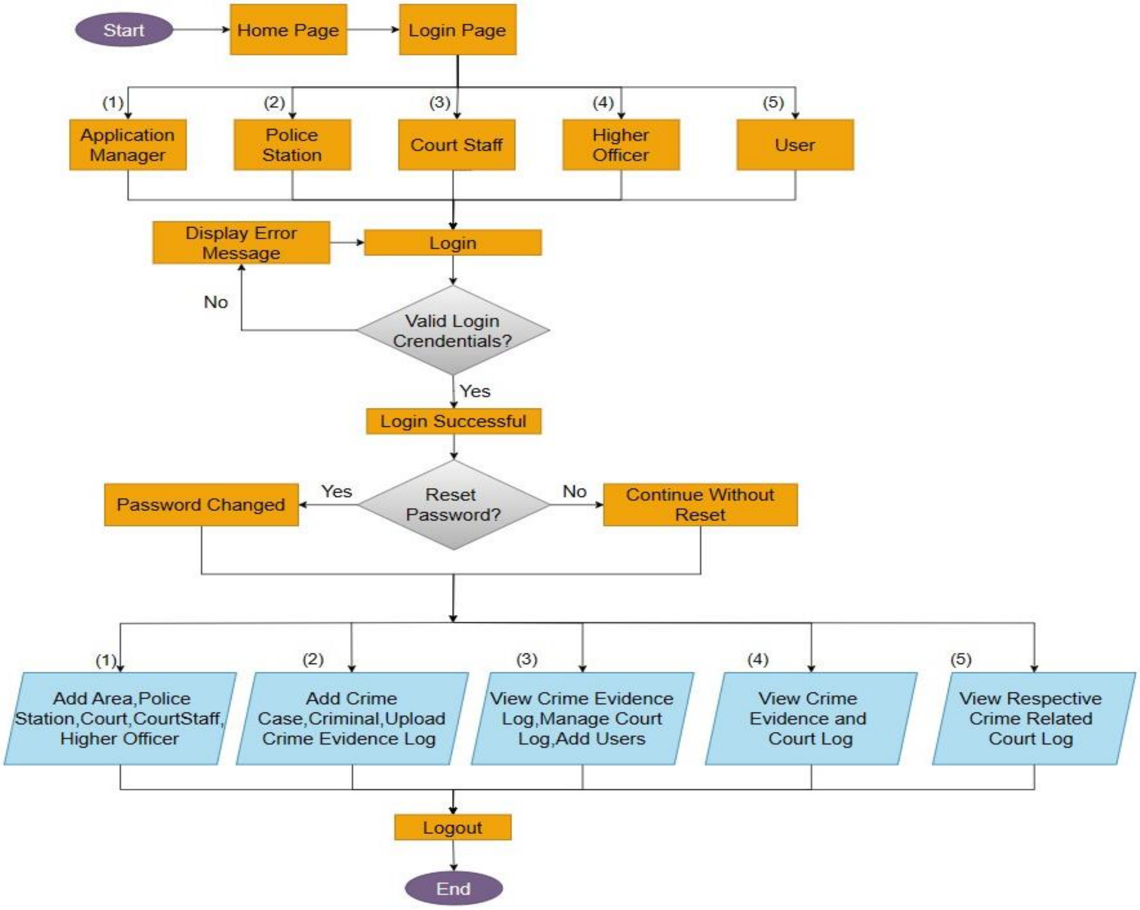
Start
Home Page
Login Page
(1)
(2)
(3)
(4)
(5)
Application Manager
Police Station
Court Staff
Higher Officer
User
Display Error Message
Login
No
Valid Login Crendentials?
Yes
Login Successful
Password Changed
Yes
Reset Password?
No
Continue Without Reset
(1)
(2)
(3)
(4)
(5)
Add Area,Police Station,Court,CourtStaff, Higher Officer
Add Crime Case,Criminal,Upload Crime Evidence Log
View Crime Evidence Log,Manage Court Log,Add Users
View Crime Evidence and Court Log
View Respective Crime Related Court Log
Logout
End

Fig -2 Flowchart

Above Fig-2 shows the flowchart of the proposed Forensic Evidence Management system. By limiting visibility to relevant stakeholders, including law enforcement officials, legal representatives, and authorized personnel, we uphold confidentiality standards while reinforcing the security and integrity of our blockchain-integrated evidence management framework. This targeted access approach not only enhances data protection but also streamlines investigative processes by facilitating secure collaboration among key stakeholder.

6. CONCLUSION & FUTURE WORK

In conclusion, the implementation of custom blockchain technology to digitalize the chain of custody from the time evidence is collected in the forensic/medical lab until it reaches the court is pivotal for ensuring the security and integrity of forensic data transactions. By maintaining a tamper-proof and transparent record of evidence handling through blockchain, a robust mechanism to track and verify the chain of custody can be established, which is paramount in legal proceedings. The utilization of custom blockchain technology allows for the seamless logging of crime evidence details onto the chain of custody, ensuring that all transactions are securely recorded and cannot be altered. Storing this blockchain-secured data in AWS S3 further enhances the security posture by leveraging AWS's reliable, scalable, and secure storage infrastructure.

The future enhancements for our forensic evidence management system aim to develop a comprehensive criminal case management system that encompasses the management of individuals involved in criminal cases, their release statuses, bail conditions, and punishments. The system will allow for tracking the progress of each case, including court dates, hearings, and judgments. Additionally, a unique identifier will be created for each individual to facilitate tracking across multiple incidents, ensuring efficient cross-referencing and analysis of patterns or repeat offenses. Furthermore, we plan to integrate a database of legal professionals, including advocates and attorneys, with details such as expertise, availability, and caseload capacity. This will enable an effective matching system to assign advocates to cases based on the nature and complexity of the crime, ensuring optimal representation. The system will also support managing advocate assignments, scheduling meetings, and tracking case progress.

7. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who contributed to the development and publication of this paper on forensic evidence management.

8. REFERENCES

[1] Alenezi, Ahmed MohanRaj, “Digital and Cloud Forensic Challenges.” ArXiv abs/2305.03059 (2023).

[2] Vadetay Saraswathi Bai, T. Sudha. (2023). “A Systematic Literature Review on Cloud Forensics in Cloud Environment”, International Journal of Intelligent Systems and Applications in Engineering (IJISAE), 11(4s), 565–578.

[3] Achar Sandesh (2022). “Cloud Computing Forensics”, International Journal Of Computer Engineering & Technology(IJECT).13.1-10.10.17605/OSF.IO/9N64K.

[4] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip and N. Singh, "An Implementation of Blockchain Technology in Forensic Evidence Management," 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE),Dubai, United Arab Emirates, 2021, pp. 208-212.

[5] S. Patil, S. Kadam and J. Katti, "Security Enhancement of Forensic Evidences Using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 263-26

[6] Mamta Khanchandani , Dr. Nirali Dave(2021), " Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects"International Journal of Scientific Research in Science and Technology(IJSRT).

[7] P. S. Murthy and V. Nagalakshmi, "Database Forensics and Security Measures to Defend from Cyber Threats," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1302-1307.

[8] S. De, M. S. Barik and I. Banerjee, "A Digital Forensic Process Model forCloud Computing," 2020 IEEE Calcutta Conference(CALCON),Kolkata,India,2020,pp.106-110.

[9] M. Chopade, S. Khan, U. Shaikh and R. Pawar, "Digital Forensics: Maintaining Chain of Custody Using Blockchain," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 744-747

[10] K. Rani and C. Sharma, "Tampering Detection of Distributed Databases using Blockchain Technology," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-4.