IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, April 2024

A Survey on 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]

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

Abstract*:* *Evidence management is crucial in the field of forensic science. Evidence obtained from a crime scene is important in solving the case and delivering justice to the victim involved. Hence, protecting the integrity of the evidence throughout the process is of prime importance. Chain of Custody (CoC) is the process which maintains the integrity of the evidence using Blockchain Technology. Inability to maintain the chain of custody will make the evidence inadmissible in court, eventually leading to the case dismissal. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchain are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Present study aims to create a framework and further propose an algorithm to implement blockchain technology to digitalize forensic evidence management system and maintain Chain of Custody.*

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

I. INTRODUCTION

Evidence management is critical in the field of forensic science. Main concern in forensic investigation is the management of evidence and documentation. Starting from the point of data extraction to till the final judgment from the court of law, maintaining the integrity of the evidence is of utmost importance. Chain of Custody (CoC) is process of documenting the evidence handled throughout the investigation in chronological order. It is essential to maintain the CoC for the evidence to be accepted in court. There are certain criteria that need to be met during the CoC procedure, such as the following: The corruption and alteration of the evidence need to be avoided to ensure its reliability. The flow of the evidence within the jurisdiction custody during the investigation process should be traceable. Presented evidence must be relevant to the crime under investigation and should serve as reliable proof. Each and every entity that has come in contact with the evidence must be able to verify the process. No unauthorized person should be allowed to deal with the evidence, to avoid any sort of alteration or manipulation of the evidence. Digitalization of forensic evidence management system saves space and at the same time makes it environment friendly and cost-efficient. Authenticity and legitimacy of CoC make evidence admissible in the court of law. These can be maintained by using Blockchain technology. Blockchain technology enables us to store various details of a system within a single network making it secure and accessible to its users. Reviewing the documents in physical format can be time consuming which can be minimized by utilizing the technology.

II. RELATED WORK

A. Chain of Custody(CoC)

Evidence is the most important aspect of any crime scene as it helps in proving guilty or innocence of the accused. Without evidence, it is very difficult to steer a case in the right direction. Proper handling and careful processing are vital in maintaining the integrity of evidence. Chain of Custody is the process of documentation of evidence from the time evidence is found at the crime scene till it reaches the court for trial. CoC plays an important role in maintaining the authenticity and credibility of evidence. It is an investigating officer's duty to ensure that only authorized person handles the evidence, and all the documentation is completed as per standard procedure. All the evidence is extracted,

DOI: 10.48175/IJARSCT-16917

processed, and stored according to established standard protocols, with the accompanying maintenance of an intact evidence log to prevent tampering of data.

B. 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.

C. 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.

D. Limitations and Challenges

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.

III. REVIEW OF LITERATURE

In paper[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. Furthermore, it advocates for the development of new approaches and technologies to ensure the admissibility of digital evidence in court.

Amidst the evolving landscape of digital forensics, researchers continually propose innovative solutions to confront the dynamic challenges of cloud forensics. The study presented in paper [2] discusses the need to analyze cutting-edge methods in cloud forensics, particularly concerning Digital Forensics and Advanced Encryption Algorithms in cybercrimes. The paper also emphasizes the importance of effectively executing frameworks for data adaptation and distribution to prevent data collection, duplication, and content tampering.

The paper [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. The rapid evolution and widespread adoption of cloud technology are driving sophisticated cloud forensic practices to address emerging challenges. While cloud innovation exacerbates existing concerns like jurisdictional issues and lack of global coordination, it also presents opportunities for innovative solutions in business, enterprise, and personal consumer use cases.

In exploring the intricacies of forensic investigations, the study presented in paper [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. Additionally, the paper suggests the development of an algorithm utilizing Hyperledger Fabric to execute the chain of custody process within the Blockchain framework

In response to the pressing need for enhanced security and transparency in forensic investigations, paper [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. Each new police complaint generates a new block in the Blockchain, allowing for accurate tracking and transparency throughout the complaint process. Any changes to a block can be traced, categorizing invalid blocks and ensuring immutability with minimal chance of alteration. Victims have real-time access to the complaint progress, further increasing transparency.

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 paper [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 paper explores various areas within cloud forensics, including the analysis of cloud service usage, effectiveness of acquisition methods, understanding commercial cloud environments, and investigating cloud forensic management.

The paper [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 Cyber security to effectively identify and analyze cyber threats. The paper advocates for strengthening various components of IT infrastructure, including networks, operating systems, database management systems, application programs, and web servers, to defend against database breaches. It underscores the necessity of implementing a suitable security policy within organizations and conducting continuous database auditing based on this policy to analyze database activity effectively.

In light of the escalating complexity and security concerns surrounding cloud networks, paper [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. This system ensures the safe transfer, recording, and updating of evidence by storing transactions securely on the Blockchain, thereby reducing overhead and tracking efforts.

In paper [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. The paper also outlines future work, which aims to maintain the Chain of Custody while storing actual evidence on IPFS and developing an end-to-end robust application.

In the quest for heightened security against cyber threats and data manipulation, paper [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. It also highlights the importance of database security and forensics, emphasizing the need for further research and application to reduce cybercrimes, frauds, and data breaches

IV. PROPOSED SYSTEM

Following Figure.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. Collaboration and enhancing the efficiency of forensic processes.

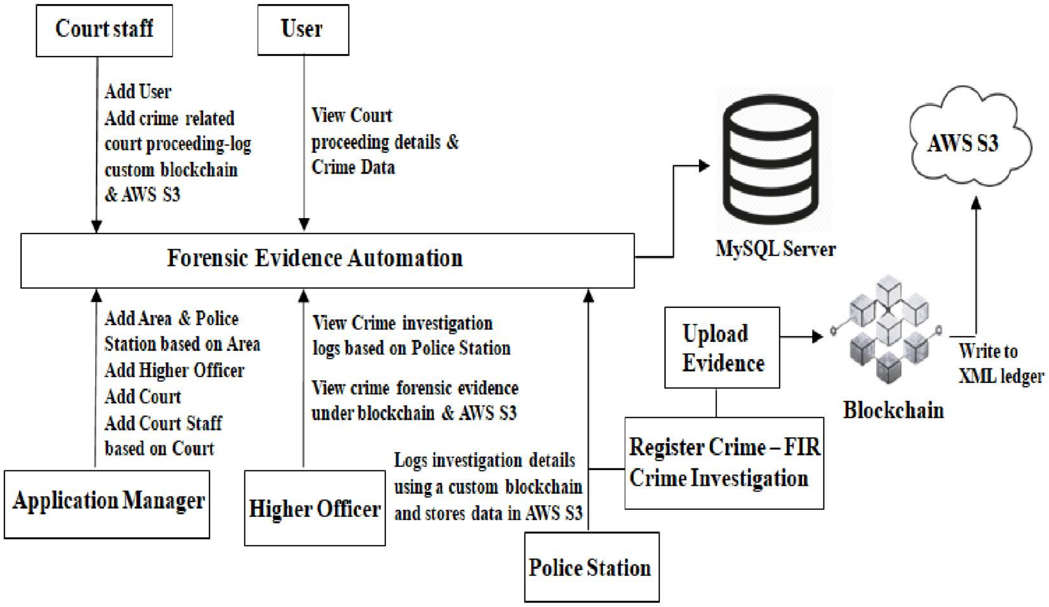

Figure 1. System Architecture

V. ACKNOWLEDGMENT

We are delighted to submit our paper titled "A Survey on Forensic Evidence Management under AWS-S3 Service" for publication. We extend our gratitude to the editorial board of the International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) for offering us the opportunity to share our research findings. Additionally, we express our appreciation to our faculty members for their support and encouragement, allowing us the chance to showcase our work. Special thanks are due to Professor Dr. Archana B for her invaluable support, guidance, and mentorship throughout this endeavor.

VI. CONCLUSION

In conclusion, the integration of both Blockchain technology and AWS S3 service into existing forensic evidence management systems offers a transformative solution to elevate the integrity, security, and transparency of handling crucial evidentiary data. Unlike traditional systems, which often rely on centralized databases susceptible to manipulation or corruption, Blockchain's decentralized and tamper-resistant nature, coupled with AWS S3's reliable and scalable storage solutions, ensures the immutability of records and mitigates the risk of data manipulation or corruption. By leveraging Blockchain and AWS S3, the existing system can significantly enhance the overall reliability of the forensic process. Furthermore, this innovation streamlines the chain of custody process, providing a seamless and transparent mechanism for tracking the custody and movement of evidence throughout its lifecycle. By fostering trust

ISSN 2581-9429 IJARSCT

DOI: 10.48175/IJARSCT-16917

among stakeholders, including law enforcement agencies, legal professionals, and the judiciary, the integration of Blockchain technology and AWS S3 service into the existing system not only enhances operational efficiency but also strengthens the foundation of justice and accountability within the forensic domain.

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 for Cloud 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.

DOI: 10.48175/IJARSCT-16917