SECURITY OF FORENSIC EVIDENCES USING BLOCKCHAIN

Prof. Kate-Deshmukh P.N*1, Tushar Bhilare*2, Rushikesh Mohite*3, Swapnil Sonawane*4, Pratiksha Wahgmare*5

*1Prof., Computer Engineering, SVPM’s College of Engineering Malegaon(BK), India.
*2,3,4,5UG Students, Computer Engineering SVPM’s College of Engineering Malegaon(BK), Baramati, India.

ABSTRACT

The current project is focused on creating and executing a comprehensive plan with the goal of accomplishing particular goals. The main goal is to use an organized and methodical approach to get a tangible result. The project's main objective is to reach predetermined milestones, and it involves several different elements, such as planning, carrying out, and evaluating. The project's scope entails strategically using resources and expertise to ensure optimal allocation for maximum efficiency. The project team's duties include working together and organizing a range of tasks, utilizing their expertise to solve problems and get beyond barriers. The project has a well-defined timeline with precise due dates for all of its phases and deliverables.

Keywords: Blockchain, Forensic Evidences, Information Security.

I. INTRODUCTION

In a number of industries, including forensic evidence management, blockchain technology has become a disruptive factor. Conventional approaches to managing and safeguarding forensic evidence frequently encounter obstacles such data modification, unauthorized access, and tampering. Blockchain provides a strong, decentralized solution that allays these worries and improves the security and integrity of forensic evidence.

DNA samples, electronic documents, and tangible artifacts are just a few examples of the diverse types of data that make up forensic evidence, which is vital to legal procedures. Data is basically unchangeable once it is recorded thanks to blockchain's decentralized structure. Every forensic evidence item is time stamped and connected to earlier recordings to create a chain of blocks. The distributed ledger technology makes guarantee that no one person or entity can control or change the information in the past tense.

The protection of forensic evidence is further strengthened by the use of smart contracts. Smart contracts are self-executing programs that, when certain requirements are satisfied, start to operate according to established rules. Smart contracts can automate the verification process in the context of forensic evidence, guaranteeing that sensitive information is only accessible to authorized persons. This improves the overall effectiveness of evidence handling while also lowering the possibility of human error.

II. LITERATURE SURVEY

Title: An Implementation of Blockchain Technology in Forensic Evidence Management.
Author: Revathy Sathyaprakasan, Pratheeksha Govindan and Samina Alvi
Description:
Forensic science relies heavily on the handling of evidence. Evidence gathered from crime scenes is crucial to wrapping up the investigation and giving the parties justice. Thus, it is critical to safeguard these evidences against tampering of any kind. The procedure that keeps the integrity of the evidence intact is called chain of custody. If the chain of custody is broken, the evidence will be excluded from the trial and the case will ultimately be dismissed. Given that it is an environmentally friendly model, it is imperative that the forensic evidence management system be digitalized. Blockchains are dispersed digital ledgers of transactions that are chronologically signed and cryptographically signed.

Author: Sonali Patil, Sarika Kadam
Description:
In the current digital era, data is crucial at every stage of the work process. Every application sector requires
the processing and storage of data with security. Because data can be altered, it must be resistant to tampering. Diverse formats can be used to represent and store data. Attacks may occur on data that is essential to a certain organization. This paper proposes a secure blockchain-based solution for forensic evidence. The Ethereum platform is used to implement the suggested scheme. Anybody in the forensic chain can readily track down instances of tampered forensic evidence. Implementing forensic evidence on the Ethereum platform with high integrity, traceability, and immutability improves its security.

**Title:**
Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology.

**Author:** Mehran Pourvahab.

**Description:**
An intelligent development of digital forensics that combats cybercrimes is cloud forensics. On the other hand, digital evidence's dependability is reduced by centralized evidence gathering and preservation. This study presents a novel digital forensic architecture for Infrastructure-as-a-Service (IaaS) cloud computing that leverages Blockchain and Software-Defined Networking (SDN), two rapidly developing technologies, to address this serious issue. The evidence in this suggested forensic architecture is gathered and stored in a blockchain that is shared by several peers. A solution called Secure Ring Verification based Authentication (SRVA) is suggested to guard against unauthorized users accessing the system. The Harmony Search Optimization (HSO) technique is used to generate secret keys in an optimal manner to fortify the cloud environment. Depending on the level of sensitivity, all data are encrypted and kept on a cloud server. With encryption, Be Aware of Sensitivity Profound Elliptic Curve.

**Title:** Blockchain Technology For Securing Foresnic

**Author:** Dr. Reshma Banu and Deeksha G

**Description:**
In today's technological world, data plays a major role in every work period. Given that data might change, it should be secure. We'll talk about data capacity and portrayal in heterogeneous organizations. Attacks against information that is vital to a particular association are possible. As cybercrime grows quickly, attackers 3 work nefariously to alter those records. Whatever the case, it's highly significant scientific evidence that supports provenance. The forensic evidence is expected to be maintained in this way since it passes through several phases during scientific analysis. In order to make the process clear, a legal chain that includes the pathology lab, forensic lab, police, and other delegates is used in this methodology to process the produced report.

**III. OBJECTIVE**
The aforementioned project's main objective is to establish and meet particular goals that are necessary for the project's overall success. The project has a defined scope and timetable and seeks to solve a specific issue, satisfy a requirement, or complete a number of tasks. This goal-oriented methodology guarantees preciseness, concentration, and quantifiable results.

Analyzing the current state of affairs or the issue that the project seeks to solve in-depth is one of the main goals. This entails compiling pertinent information, recognizing significant obstacles, and comprehending the environment in which the project will function. The basis for well-informed decision-making and efficient planning is laid by this first action.

Creating a precise project scope that defines the parameters and restrictions of the endeavor is another essential goal. This entails specifying the project's deliverables, benchmarks, and essential elements. Throughout the execution phase, the project team and stakeholders are guided by a clearly defined scope that serves as a roadmap.

**IV. PROPOSED SYSTEM**
The incorporation of blockchain technology is one suggested method to improve the protection of forensic evidence. Blockchain can offer a transparent and safe framework for handling forensic data since it is a decentralized, tamper-resistant ledger. Under this method, every piece of forensic evidence is registered on the
blockchain and given a unique number. The evidence’s digital fingerprint is connected to this identifier, protecting its integrity and thwarting unwanted changes. Blockchain is immune to tampering because it is decentralized; any effort to alter data on one node would be instantly visible to all nodes in the network.

On the blockchain, self-executing programs known as "smart contracts" can be used to automate and enforce chain-of-custody rules. These agreements minimize the possibility of corruption or tampering by guaranteeing that only authorized individuals can access and transfer evidence data. Furthermore, blockchain timestamps offer an unchangeable documentation of the exact moment of every transaction, assisting in the establishment of the chronological sequence in which evidence is handled.

Cryptographic keys can be used to establish access controls, restricting data access to individuals who are permitted, such as law enforcement, forensic specialists, and investigators. This guarantees that only authorized personnel can contribute to or evaluate the forensic data, safeguarding the privacy of sensitive information in the process.

V. SYSTEM ARCHITECTURE

VI. CONCLUSION

In conclusion, employing blockchain technology in forensic evidence management enhances the security and integrity of crucial legal information. The decentralized and tamper-resistant nature of blockchain ensures that once data is recorded, it becomes virtually immutable, reducing the risk of unauthorized alterations or deletions. This characteristic is particularly significant in the context of forensic evidence, where the accuracy and reliability of data are paramount for legal proceedings.

By leveraging blockchain, forensic evidence undergoes a transparent and traceable lifecycle. Every transaction, from the initial collection of evidence to its analysis and presentation in court, is securely recorded on the blockchain. This transparency not only ensures accountability but also facilitates the establishment of a clear chain of custody. Legal professionals and investigators can easily trace the entire history of a piece of evidence, reinforcing its authenticity and admissibility in court.

ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Kate-Deshmukh P. N. and Head of the Department Prof. Dr. Sinkar Y. D. and Hon. Principal Prof. Dr. Mukane S. M. for their valuable guidance and for providing all
the necessary facilities which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Computer Engineering of SVPM’s College of Engineering, Malegaon(Bk) for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

VII. REFERENCE


