Screening Forensic Evidence Employing Blockchain

[1]Ashitha C A, 2Asik Anwar M N, [3]Fathima Shani, [4]Rizwanul Haq, [5]Chithra Rani P R

[1,2,3,4]B. Tech Student, [5]Assistant professor
Department of Computer Science and Engineering,
Ilahia College of Engineering and Technology
Muvattupuzha, India.

***Abstract*- Data is essential for helping firms find the source of issues and comprehend the connections between various divisions, systems, and places. Data must also be correct in order to accurately characterize, calibrate, verify, validate, and analyze the performance and long-term durability of materials in harsh settings. Nonetheless, data security continues to be a major worry, particularly when it comes to crucial data that enterprises must defend from prospective assaults. We suggest a safe method that makes use of blockchain technology to protect forensic evidence in order to solve this problem. Our solution is built on the Ethereum platform, making it simple for anyone in the forensic chain to track down any evidence that has been tampered with at any point. We assure the security of our systems by implementing high integrity, traceability, and immutability.**

The implementation of the Blockchain-based system secures forensic reports. By establishing a chain of confined users who are accountable for the inquiry, the secure forensic evidence system has been developed to accomplish optimization. For the purposes of achieving transparency and immutability, they are each given their own access. Blockchain improves the traceability, security, trustworthiness, and transparency of data shared across a business network while generating new efficiencies that save costs. Blockchain for business employs an open, unchangeable ledger that only members with authorization can view. Empower users to own their data by giving them access to both private and public keys. It is not permitted for third-party intermediaries to obtain and misuse data.

***Index Terms*- Information Security, forensic evidence, Blockchain Technology.**

I. INTRODUCTION

The implementation of a blockchain-based system has been proposed to secure forensic reports and optimize the investigation process. The system involves creating a chain of limited users who are responsible for the investigation, and they are given respective access to achieve transparency and immutability. Blockchain forensics is utilized to interpret the flow of digital assets by taking data from the blockchain, which is an assortment of connected blocks that track all activities occurring on a distributed system. In today's dynamic era of continuous cybercrime, there is a fundamental need for advanced proof to verify the origin and connection associated with cybercrime. However, online proof faces several challenges, including break of integrity and denial during the exchange of digital evidence. To solve this problem, a chain of custody is described as a system used to store and record the original history of the processing of digital evidence. This ensures accountability, reliability, security and auditing of the system. Blockchain technology offers four key features, including a public distributed ledger or decentralization, hash encryption, proof of work or transparency, and miners. The technology uses hashing and encryption to protect data and provides a reliable and secure evidence platform for cybercrime investigations.

Currently, the police department has various online systems that facilitate the registration of complaints and keep a record of allcases at the respective police department. However, there are some limitations on traceability, transparency, immutability, and complete system security. These shortcomings reduce the credibility of the system and impede complaint resolution, resulting in abacklog of pending cases that can last for years. Furthermore, the prevalence of fraudulent practices can falsify important data, reducing system reliability and preventing people from filing complaints. To address these issues, there is an urgent need to developa robust system that provides full traceability, transparency and security, thereby ensuring that complainants can receive updates ontheir claims at any time. In addition, the system should enforce the timing of cases, ensure that police are accountable, and handle complaints in a timely and efficient manner.

Securing evidence is critical to ascertaining the truth because forensic evidence is subject to damage, alteration, or destruction through improper handling or examination. It is important to preserve the integrity of evidence and ensure its admissibility in court. Blockchain technology can ensure the immutability and integrity of stored evidence data. In addition, the storage of digital evidence between the nodes of the court participants eliminates the risk of failure of the centralized storage server. Each new block is linked to all previous blocks in a cryptographic chain, making it nearly impossible to break. Additionally, a consensus mechanism verifies and agrees all transactions within blocks to ensure their accuracy and authenticity.

II. RELATED WORKS

The purpose of this literature survey is to analyze and providing the means to secure forensic evidence using blockchain. Specifically, we focus on the papers that propose different approaches for preventing tampering of data in digital world. We compare and contrast the various techniques used for forensic evidence security, such as NAND flash memory, selective deletion, and video/image enhancement. The literature survey compares and contrasts the different approaches proposed by the researchers, highlighting the strengths and weaknesses of each technique. We analyze the various factors that influence the effectiveness of the

proposed systems, such as the accuracy of the security algorithms, the complexity of the security algorithms, and the ease of implementation.

The paper "Simulation Research of Crime Scene Based on UDK" they say that the sence simulation is an important branch of virtual reality and is an indispensable high-tech means for the development of various areas in society. It provides a software accessto simultaneous application of graph and high fidelity and multichannel. In this paper, the prominent merits are used to solve above problem, such as real-time visual simulation, easy programming, short period of development, flexible application, powerful function and so on. The visual simulation and forensic science were closely integrated through the invasive interaction between the user and the simulation environment. Finally, this paper takes a murder case as an example and finds a new solution for the problem of scene investigation and reconstruction.

The paper "Automatic, Selective and Secure Deletion of Digital Evidence" they focus on the importance of secure deletion for user privacy and Digital Forensics purposes. The key concept is that erasing data from digital devices is not a simple task, since some inherent characteristics of digital systems can retain recoverable information about it (i.e., data remanence). In substance, data remanence can be considered a problem to solve in order to grant user privacy in many situations where secure deletion is crucial, as well as a benefit to exploit to gain useful evidence in a digital forensics analysis. And describes a methodology to delete a predetermined data set from a digital device in a secure and fast way, for example, with a single click of the mouse. All the actions required to remove the unwanted evidence can be performed by means of an automation, which is also able to remove traces about its execution and presence on the system. A postmortem digital forensics analysis of the system will never reveal any information that may be referable to either the deleted data set or automation process.

The paper "A sample of Digital Forensic Quality Assurance in the south African Criminal Justice System" they focus on the Digital evidence. Digital evidence is now a fundamental part of many investigations. Digital evidence is defined as information ofa legal probative value that is either stored, or transmitted, in a digital form. As a forensic science, digital forensics has the power to persuade in a court of law, and as such it is crucial that the courts assess the validity of a scientific process before accepting its result. A key factor in any court case, especially a criminal one, is the importance of quality evidence. This is especially important when considering that the standard of proof which must be satisfied to obtain a conviction in a criminal court is beyond a reasonable doubt, and where evidence that is not considered quality evidence may be enough to create reasonable doubt of guilt. The quality of evidence is crucial to ensure that criminal perpetrators are not only brought before court and prosecuted. In the case of digital evidence, which is fragile by its very nature, special attention and care needs to be taken to ensure that it will be accepted in court. Digital forensics, which is the forensic science defined by, has a symbiotic relationship with digital evidence, where digital evidence often depends on digital forensics for use in court.

The paper "Design and Implementation of a Cloud Based Forensic Science Information System Model" they propose a Cloud Based Forensic Science Information System. In the past, forensic science management team has stored records of their forensic science information on paper. They had to ensure that this data is private and secure by keeping the paper records in a locked filingcabinet. With increased use of personal computers and modern information technology in forensic science, there are easy ways to manage the electronic records in the system frame is based on C/S. But nowadays, outsourcing of cloud computing leads to a complex system where the information data can store and process at many different places. The utilization of cloud-based models can significantly reduce costs and improve resource utilization for Forensic Science Information Management Systems. The purpose of the system design is to eliminate heavy manual work and thereby increase work efficiency. Compared to traditional design schemes, this system provides easy and comprehensive access to forensic data in the cloud and opportunities to use the services offorensic experts who may be located in remote locations. Therefore, plays an important role in the development of cloud-based forensic information system.

The paper "Automatic Timeline Construction and Analysis for Computer Forensic Purposes" they present a multi-layered architecture to automatically perform event reconstruction, from data extraction to table analysis through construction, and assist the investigation team in extracting data from the remaining data. Crime scene, creation of an incident report table and recent interpretation. A feature of this architecture is the use of a knowledge representation model that allows rich semantic information about events, such as the resources they use or the participants in them, to be stored. This knowledge is then used for investigators with advanced analysis and visualization.

The paper "Digital Forensic Analysis for Enhancing Information Security" they simulate digital crime scenarios and conduct forensic analysis to improve security. To accomplish this, this document uses several forensic techniques and countermeasures. Analyzed data were obtained from the simulation results. The results of show that although the investigation of digital crimes is difficult, it can be achieved with the help of sophisticated forensic / counter-forensic tools.

The paper "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation" they develop advanced forensic video analysis techniques to assist the forensic investigation. They first propose a forensic video analysis framework that employs an efficient video/image enhancing algorithm for the low quality of footage analysis. Introducing an adaptive video enhancement algorithm that employs contrast limited adaptive histogram equalization (CLAHE), which aims to enhance the quality of closed-circuit television (CCTV) footage specifically for digital forensic investigations. To assist the video-based forensic analysis, a deep learning-based object detection and tracking algorithm are proposed that can detect and identify potential suspects and tools from footages. In the past few years, the 'image enhancement' techniques have been proposed, most of them can be grouped into spatial domain methods and frequency domain methods. These methods show good potential for improving image quality, but only some of them can be used for low-quality footage, such as CCTV footage, mobile clips, etc.

The paper "MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture" they use blockchain technology to create a secure and transparent process for digital forensic investigations, which fills the current gap. A new architecture is proposed, called MF-Ledger, which uses Hyperledger Sawtooth to ensure security and efficiency. In this architecture, participating stakeholders establish a private network to collaborate and reach

agreements on various investigation activities, which are then recorded on the blockchain ledger. They have created digital contracts (smart contracts) and implemented them using sequence diagrams to handle the stakeholders' secure interaction in the investigationprocess. The architectural solution proposed provides a strong mechanism for information integrity, prevention, and preservation, ensuring that evidence (including chain of custody) is permanently and immutably stored on a private, permissioned, and encryptedblockchain ledger. To ensure the validity, authenticity and reliability of digital forensic investigations, it is imperative and extremelysignificant to maintain the transparency and secrecy of the whole digital forensic investigation process. In order to ensure the integrity of the evidence, it is essential to preserve and protect it in a secure container and store it in a reliable locker where it cannotbe tampered with. It is substantial to highlight that only original and non-tempered evidence that is authentic, comprehensive, trustworthy with a complete chain of custody is only adequate and admissible in the court of law. However, the current traditional digital forensic process lacks standardized procedures and mechanisms, making it inherently vulnerable to various tampering and forgery occurrences against the recent cybercrime incidents. Such incidents typically occur due to the continuous technological advancements and lack of knowledge and expertise at the forensic expert level when they are collecting, storing and analyzing the forensic evidence for a particular cybercrime use case.

The paper "Blockchain Solution for Forensic Evidences Preservation in IoT Environments" they propose an innovative blockchain-based solution for collecting and preserving digital forensic evidence in the smart home domain. The system uses a private forensic evidence database to store captured evidence and a permissioned blockchain to provide security services such as integrity, authentication, and non-repudiation. This ensures that the evidence can be used in court. The storage of metadata about evidence on the blockchain is crucial for facilitating related services. Additionally, the blockchain interacts with various entities involved in the investigation process, such as Internet service providers, law enforcement agencies, and prosecutors, through the use of smart contracts. The paper also presents a high-level architecture of the blockchain-based solution, which addresses the unique challenges posed by the need to handle digital forensic evidence from IoT networks

The paper "An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash" they use a method that is sufficiently efficient and convenient procedurally, but the integrity of prospective evidence may be jeopardized if the central authority is attacked by a malevolent attacker. Additionally, human and material resources are expended to maintain the chain of custody and ensure the investigation's integrity. Unlike today, the existing chain of custody method must include a more robust approach to integrity preservation and streamlined processes in order to conduct a thorough digital forensic investigation in large scale IoT settings. They performed a preliminary forensic study on the blockchain-based forensic investigation framework, taking into account the variety of devices, evidence items, and data formats found in the complex IoT environment. They propose a blockchain-based digital forensic framework for the IoT environment in this article to address the heterogeneity and dispersion of the IoT environment, as well as the centralization of current forensic investigations. In addition, they show the updated structure of the block and the workflow of the proposed framework for encoding Merkle trees with a fuzzy hash for similar proof processing (various version document).

The paper "Security Enhancement of Forensic Evidences Using Blockchain" they propose a secure system for forensic evidences based on blockchain technology, which is implemented on the Ethereum platform. The system ensures that any tampering with the forensic evidence can be traced easily at any stage by anyone in the forensic chain. By implementing the system on Ethereum, the security of forensic evidence is enhanced with high integrity, traceability, and immutability. The proposed system is used to accurately track police complaints with an increased level of belief and a decreased level of conflict. Whenever a new complaint is raised, a new block is added to the blockchain, and any change to that block can be traced. Invalid blocks are categorized, ensuring a very rare chance of immutability.

III. PROPOSED SYSTEM

In the proposed system we a website to secure forensic evidences using the technology of blockchain. data can be altered easilyit is necessary to secure the data which is the basis for every organization. here we suggest an Ethereum platform. Ethereum offersan extremely flexible platform on which to build decentralized applications using the native Solidity scripting language and Ethereum Virtual Machine. Decentralized application developers who deploy smart contracts on Ethereum benefit from the rich ecosystem of developer tooling and established best practices that have come with the maturity of the protocol. This maturity also extends into the quality of user-experience for the average user of Ethereum applications, with wallets like MetaMask, Argent, Rainbow and more offering simple interfaces through which to interact with the Ethereum blockchain and smart contracts deployed there. Ethereum's large user base encourages developers to deploy their applications on the network, which further reinforces Ethereum as the primary home for decentralized applications like DeFi and NFTs. In the future, the backwards-compatible Ethereum 2.0 protocol, currently under development, will provide a more scalable network on which to build decentralized applications that require higher transaction throughput.

There is a high chance of risk for saving everything in the database as there is no security in order to overcome these obstacles,we are implementing the system with block chain. There will be only one login and two staffs. One staff is assigned by the admin toadd details about the forensic. Second staff is the admin itself but will be anonymous and verify the details given by the staff.

Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data. Transactions are sent from and received by user-created Ethereum accounts. A sender must sign transactions and spend Ether, Ethereum's native cryptocurrency, as a cost of processing transactions on the network.

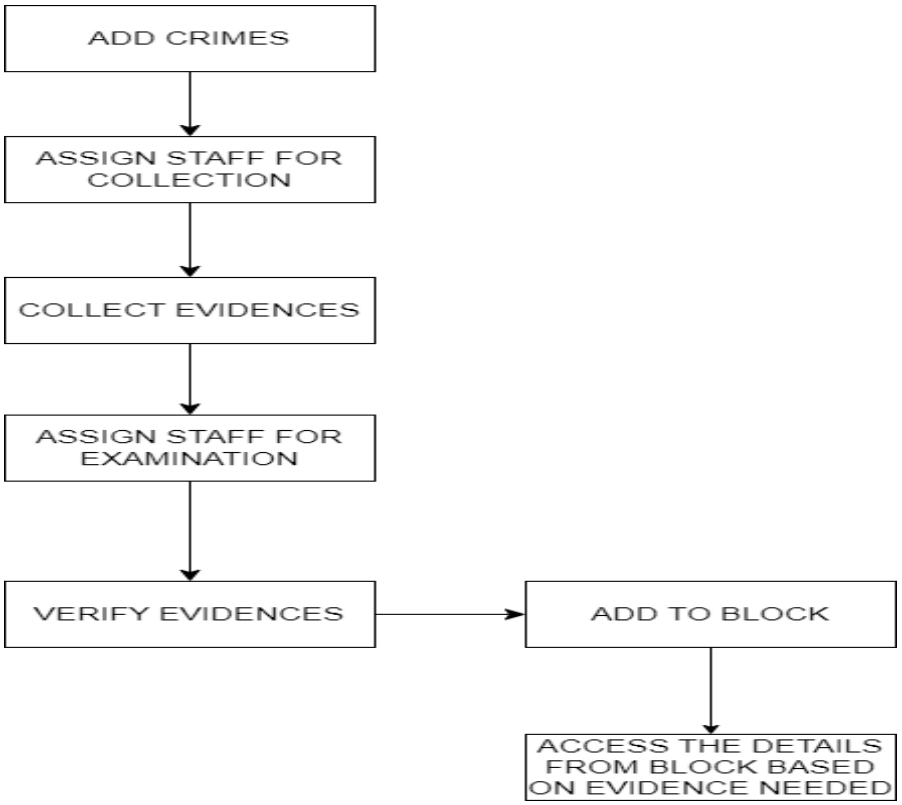

Fig. 1. Architecture of proposed system

IV. MODULES

A. Admin

To access the website, the admin must provide a valid username and password. Once logged in, the admin has various permissions, such as adding or deleting staff, viewing police records, court documents, and criminal activities, and assigning staff to collect and examine evidence. Additionally, the admin can view court requests for evidence and choose to accept or reject them as needed. These options give the admin greater control and oversight over the operations of the website, making it a valuable tool for managing and maintaining the integrity of the system.

B. Staff

The staff members are provided with the option to log in to their account using their unique username and password. Upon successful validation of the credentials, the staff can access various features such as editing their profile, viewing assigned cases, collecting and verifying evidence, and marking their attendance. However, if the login credentials are invalid, the staff members willnot be able to access these features.

C. Police Station

To ensure secure access to the website, the police station is required to provide a valid username and password when logging in.Once authenticated, they are granted specific privileges, including the ability to register stations, add and view crime records, and view evidence. However, if the login credentials are invalid, they will not be able to proceed with accessing the website. This systemis designed to maintain the integrity of the website and restrict access to authorized personnel only.

D. Court

To access the features of the platform, the court is required to enter a valid username and password during login and logout sessions. Once authenticated, the court can perform various tasks such as requesting court registration and viewing evidences relatedto a case. However, without valid login credentials, the court will not be able to access these features.

V. FUTURE SCOPE

The Blockchain based system is implemented for securing forensic reports. The secure forensic evidence system has been proposed to achieve optimization by creating chain of limited users responsible in the investigation. Blockchain forensic stakes data

from the blockchain to interpret the flow of digital assets. Data is secured using blockchain, we need to access the details only by providing various contents. To overcome this, QR code is provided where the details is given under. The blockchain technology can offer forensic applications with substantial benefits for the whole procedure of digital forensics investigation procedures, including the data collection, preserving, evidence validating, data analysis, and the Presentation increases trust, security, transparency, and the traceability of data shared across a business network of the finding. In order to provide further security, various encryption and description method is implemented.

VI. CONCLUSION

Blockchain technology's data structures have inherent security qualities because they are based on consensus, cryptography, and decentralization principles. Each new block of information connects to all the previous blocks in a way that it's nearly impossible to tamper with Digital forensics can be implemented on Ethereum platform, provides high security, high integrity, high mutability. Forensic evidences are secured which serves the basic for digital forensic. Third-party intermediaries are not allowed to misuse and obtain data, creating a permanent and immutable record of transaction. Blockchain facilitates the verification and traceability of multi-step transactions that require such functions. It can speed up data transfer procedures, offer secure transactions, and lower compliance expenses. Blockchain technology can facilitate contract management and verify a product's provenance. Users of forensic reports must comprehend the conclusion and the strength of the conclusion's evidence in order to properly evaluate the evidence. In conclusion, forensic science's capabilities are admirable.

VII. ACKNOWLEDGMENT

Apart from the effort of us, the success of this project preliminary report depends largely on the encouragement and guidelines of many other. We take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project. We would like to show my heartfelt gratitude towards Prof. DR K A NAVAS, Principal, Ilahia College of Engineering and Technology for granting me the permission to work this project. Also, we would like to show my greatest gratitude towards our head of department of Computer Science & Engineering Dr. Lino Abraham Varghese and project guide Ms. Chithra Rani P R and project coordinator Ms. Chithra Rani P R, Mr. Shanavas K A for their valuable advice and guidance. Finally, we express my gratitude and thank to all our teachers and other faculty members of the department of Computer Science & Engineering, for their sincere and friendly cooperation in completing this project.

REFERENCES:

1. Sonali Patil, Sarika Kadam, Jayashree Katti "Security Enhancement of Forensic Evidences Using Blockchain" IEEE 2021.
2. Ojeniyi Joseph Adebayo, Idris Suleiman, Abdulmalik Yunusa Ade, Ganiyu, S. O, and Alabi, I. O "Digital Forensic Analysis for Enhancing Information Security " IEEE 2015.
3. Na Li,Yanhui Du "Design and Implementation of a Cloud Based Forensic Science Information System Model" IEEE 2013.
4. Yoan Chabot∗, Aurelie Bertaux∗, Christophe Nicolle∗ and Tahar Kechadi† "Automatic Timeline Construction and Analysis for Computer Forensics Purposes" IEEE 2014.
5. JIANYU XIAO, SHANCANG LI, (Member, IEEE), AND QINGLIANG XU "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation" IEEE 2019.
6. Aniello Castiglione∗, Giuseppe Cattaneo†, Giancarlo De Maio‡, Alfredo De Santis§ "Automatic, Selective and Secure Deletion of Digital Evidence" 2011.
7. WAEL A. MAHROUS, MAHMOUD FAROUK, AND SAAD M. DARWISH "An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash" IEEE 2021.
8. Jason Jordaan "A Sample of Digital Forensic Quality Assurance in the South African Criminal Justice System" IEEE 2012.
9. Xu Feng, Shan Daguo, Yang Hongchen "Simulation Research of Crime Scene Based on UDK" IEEE 2010.
10. NA YOUNG AHN AND DONG HOON LEE, (Member, IEEE) "Security of IoT Device: Perspective Forensic/Anti-Forensic Issues on Invalid Area of NAND Flash Memory" IEEE 2022.
11. Sotirios Brotsis∗, Nicholas Kolokotronis∗, Konstantinos Limniotis∗, Stavros Shiaeles†, Dimitris Kavallieros‡, Emanuele Bellini§, and Cl´ement Pavu´e¶ "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments" IEEE 2019.
12. Dr. S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree, A. Gayathri, V. Jebin Andrews "Digital Forensics Using Blockchain". International Journal of Recent Techonology and Engineering (IJRTE) ISSN: 2277-3878, Volume 8.
13. Maria Stoyanova, Yannis Nikoloudakis , Spyridon Panagiotakis , Evangelos Pallis, and Evangelos K. Markakis."A Surveyon the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues". IEEE 2020.
14. https://www.analyticsinsight.net/all-you-need-to-know-about-blockchain-forensic-for-crypto-crimes/#:~:text=Blockchain%20forensic%20is%20the%20emerging,and%20transparent%20blockchain%20digital%20le ader.
15. Dr. Reshma Banu, Deeksha G, M Preethi, Triveni S. "BLOCKCHAIN TECHNOLOGY FOR SECURING FORENSIC EVIDENCE". International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org, ISSN: 2320-2882, Volume 10.
16. https://aws.amazon.com/what is/blockchain/#:~:text=Blockchain%20technology%20is%20an%20advanced,linked%20together%20in%20a%20chain.
17. https://link.springer.com/chapter/10.1007/978-3-030-27798 7_15#:~:text=Blockchain%20technology%20creates%20a%20permanent,theft%2C%20and%20information%20loss%20i mpossible.
18. https://www.careerera.com/blog/future-scope-of-block-chain technology#:~:text=For%20apparent%20reasons%2C%20the%20future,vulnerabilities%20like%20illegal%20data%20ta mpering.
19. https://ieeexplore.ieee.org/document/8592253/.