IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

PRESERVING INTEGRITY OF FORENSIC EVIDENCE USING BLOCKCHAIN TECHNOLOGY

DURGALAKSHMI P
STUDENT
CSE DEPARTMENT
IFET COLLEGE OF ENGINEERING,
VILLUPURAM, TAMILNADU

DIVYA M
ASSISTANT PROFESSOR
CSE DEPARTMENT
IFET COLLEGE OF ENGINEERING,
VILLUPURAM, TAMILNADU

Abstract : The application of blockchain technology to forensic investigations is a major advancement for the criminal justice and legal systems, resolving important issues and utilizing smart contracts to protect and automate crucial investigative procedures. The integration of blockchain technology in forensic investigations not only signifies a major advancement but also addresses several critical challenges faced by the legal and criminal justice system. At the heart of this integration are smart contracts, which automate and secure key aspects of the investigative process. These self-executing agreements operate with predefined rules and conditions, ensuring the utmost integrity and transparency in crucial tasks such as evidence tracking, chain of custody management, and access control. One of the primary benefits of this system is the substantial enhancement of data security. Blockchain's foundation in cryptographic principles and decentralized architecture makes it exceptionally resistant to unauthorized access and tampering. This level of security is particularly vital in forensic investigations, where maintaining the integrity of evidence is paramount. Furthermore, the immutability of blockchain records is a game-changer in ensuring the reliability of information. Once data is recorded on the blockchain, it becomes virtually impossible to alter, offering an unchangeable ledger of events and actions throughout the investigation. In summary, this innovative integration of blockchain and smart contracts delivers heightened efficiency, traceability, and transparency to the forensic investigation process. It not only safeguards the integrity of evidence but also streamlines operations, reducing the potential for errors and disputes. By providing an unforgeable and transparent chain of custody and evidence history, this system significantly strengthens the overall quality and trustworthiness of forensic investigations within the legal and criminal justice framework

KEYWORDS: Blockchain, Chain of Custody, Digital evidence, Blowfish, Image Forensic

I INTRODUCTION

In cyberattack investigations, forensic intelligence entails the methodical gathering, preserving, and inspection of digital evidence by trained forensic investigators. By adhering to stringent forensic principles and procedures and preserving an uninterrupted chain of custody that is essential for legal proceedings, these professionals guarantee the integrity of the evidence. The examination phase starts after the evidence has been seized. Specialized tools are used to create a copy of digital data, keeping the original safe for evidence and enabling forensic analysis. Experts examine imaged data while closely collaborating with clients, looking for critical information such as erased files, attack detection, and digital activity reconstruction. An important part of the analysis process is finding the guilty parties and gathering proof for court cases. To extract actionable intelligence from the data, one must possess technical proficiency, meticulousness, and in-depth knowledge of digital forensic techniques. crucial for legal proceedings.

Forensic intelligence plays a critical role in modern investigative processes, particularly in the context of cyber-attacks and digital crimes. It encompasses a range of techniques and methodologies to gather and analyze evidence both before and after these incidents occur. A key component of this discipline is the expertise of forensic investigators who are trained to safely preserve and examine data on digital devices and networks. Their primary objective is to identify the root causes of incidents and gather evidence essential for legal proceedings. In conducting digital forensic investigations, it is imperative to adhere to established forensic principles, evidence continuity, and rigorous methodologies. This ensures that the integrity and admissibility of the evidence collected are maintained throughout the investigative process. Forensic investigators are well-versed in the legal aspects, best practices, and methodologies prevalent in the contemporary digital forensic intelligence environment. Evidence continuity, a foundational concept in this field, encompasses a comprehensive approach covering the entire lifecycle of digital evidence.

II NEED OF THE STUDY.

In the realm of cybercrime investigations, digital evidence is the cornerstone upon which cases are built. However, digital evidence poses several significant challenges. It is complex, highly volatile, and, critically, susceptible to manipulation. Ensuring the integrity of this evidence is paramount to establishing trust in the legal process. A key aspect of this assurance is the Chain of Custody (CoC), a meticulous record of the handling and transfer of digital evidence from the moment it's collected to its use in court. The CoC attests that the evidence has not been tampered with during its journey .The problem, however, lies in the inherent uncertainty surrounding digital evidence. Technologies used in cybercrime investigations are not infallible and can introduce errors and inaccuracies into the process. These uncertainties make it challenging to definitively determine the trustworthiness of digital evidence, potentially casting doubt on the outcomes of investigations and legal proceedings

A. IPFS

The InterPlanetary File System, or IPFS for short, is a peerto-peer network and protocol that was developed to provide a distributed file system with a decentralized approach to storing and sharing hypermedia. Instead of acting as a conventional server, it functions as a network in which a collection of hashed files is stored on each node. Alternatively, users can run an IPFS node that hosts content if they want to use IPFS more like a server. Using IPFS, the node would be in charge of file distribution and storage. By uploading files to their local IPFS node and then accessing these files via the node's distinct hash, users can contribute content to the IPFS network. The procedure entails launching an IPFS daemon on the server, allowing other IPFS network nodes to store and retrieve content. This functions similarly to a server by efficiently serving content to those who request it. While IPFS can operate in this distributed fashion, it is important to remember that it is fundamentally different from a centralized server in that the content is hosted in a peer-topeer fashion across multiple nodes.

B. Advantage of the IPFS Server

IPFS (InterPlanetary File System) offers several advantages, particularly in the context of data storage and distribution, making it an appealing solution for various use cases:

Decentralization: IPFS is built on the principles of decentralization, meaning data is distributed across a network of peers rather than being reliant on centralized servers. This reduces the risk of a single point of failure and enhances data availability.

Censorship Resistance: Because data is distributed across a peer-to-peer network, it is inherently more resistant to censorship. This is particularly valuable in regions where internet access and content may be restricted.

Content Addressing: IPFS uses content addressing, where data is identified by its unique cryptographic hash. This ensures data integrity and simplifies data retrieval. Changes to the data result in a different hash, making it tamper-evident.

Blockchain Integration: IPFS can be used in conjunction with blockchain technology to ensure the permanence and integrity of data, which is beneficial for various applications, including decentralized finance (DeFi) and supply chain management.

Open Source: IPFS is open-source, fostering collaboration and innovation, and allowing for its use in a wide range of projects and applications.

IPFS is an evolving technology with a growing ecosystem, and its advantages make it a compelling choice for scenarios where decentralized, secure, and efficient data distribution is a priority.

collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

C. BlowFish Algorithm

In 1993, Bruce Schneier introduced Blowfish as a significant and compelling alternative to the Data Encryption Standard (DES). Blowfish garnered attention for its notable improvements, particularly in terms of speed, offering a commendable encryption rate. One of its most remarkable attributes is the robust security it provides. Notably, as of now, no effective cryptanalysis technique has successfully compromised Blowfish's encryption, underlining its reputation as a secure method for safeguarding data.

One of the key advantages of Blowfish lies in its open and freely accessible nature. It was among the early block ciphers that were not subject to any patents, making it available for a broad spectrum of users, including developers and organizations. This open availability has contributed significantly to its widespread use in various applications.

Blowfish operates as a symmetric block cipher algorithm, meaning it uses the same key for both encryption and decryption. Its continued relevance in the world of cryptography underscores its value in efficiently and securely encrypting data. Whether used for securing sensitive communications, protecting files, or enhancing the security of digital systems, Blowfish remains a valuable and trusted tool in the field of encryption.

III LITERATURE SURVEY

A permissionless blockchain privacy-preserving solution is suggested, addressing on-chain data privacy issues while emphasizing user control over transaction data. Ethereum smart contracts and symmetric cryptography are used in the system. Authorized users are listed in an access control list by data providers, and data consumers can check this list to confirm the legitimacy of the users. Data consumers can ask data providers for a security key to access private information after successful validation. The key for access issent through an executed smart contract between the data provider and the consumer. The Ropsten test network is used to assess the performance of these smart contracts, which are implemented in Solidity[1]. Stakeholders can establish a private network with MF-Ledger to enable safe and open digital forensic investigations. A variety of investigation activities are agreed upon and exchanged amongst participating stakeholders prior to being recorded on the blockchain ledger. Sequence diagrams are utilized in the implementation of digital contracts, which are also referred to as smart contracts, to facilitate secure interactions between stakeholders while conducting investigations. Strong information integrity, prevention, and preservation features are provided by this architectural solution, guaranteeing the long-term, unchangeable storage of evidence (including the chain of custody) inside a private, permission-only, encrypted blockchain ledger. To put it succinctly, MF-Ledger solves the changing problems presented by the contemporary digital environment while improving the security and reliability of digital forensic investigations in the field of multimedia [2]. This work presents a novel framework for blockchain-based digital 2 forensics (DF) investigations designed for social systems and the Internet of Things (IoT). Through the assurance of authenticity, immutability, traceability, resilience, and distributed trust among involved parties, it provides proof of existence and privacy preservation for evidence examination. To ensure traceability and provenance tracking, IoTFC logs information about the identification, preservation, analysis, and presentation of evidence in blockchain blocks. Examiners and evidence items alike benefit from IoTFC's transparency in the audit trail. The paper also addresses the use of blockchain technology for private key-based message signing and secure communication in defense applications. Overall, the decentralized features of blockchain technology complement DF's requirements for preserving the traceability and integrity of evidence in a variety of settings and applications[3] The methodology section outline the plan and method that how the study is conducted. This includes Universe of the study, sample of the study,Data and Sources of Data, study's variables and analytical framework. The details are as follows;

IV EXISTING SYSTEM

A. Fuzzy Hash:

Digital evidence is a crucial element in cybercrime investigations, frequently acting as the connecting thread to establish connections between suspects and illegal activity. Digital evidence, however, is a dynamic and complex object that can be altered and manipulated. In order to guarantee the authenticity of this evidence, the chain of custody (CoC) is essential. The Chain of Custody (CoC) is an organized procedure that tracks and documents the handling of digital evidence, assisting in the verification that it hasn't been altered while being investigated. The use of fuzzy hash functions in a blockchain environment is the main innovation. In doing so, the system makes it possible to evaluate the integrity of digital evidence in a more flexible and nuanced manner. It adds the ability to measure the degree of image dissimilarity, which is useful in forensic situations. This improvement—which is illustrated by image forensics—addresses the inherent uncertainties that frequently surround digital evidence and adds to the overall trustworthiness of CoC documents. The investigation process is essentially made more transparent and sophisticated by this method, which also strengthens the validity of digital evidence and, in the end, the pursuit of justice in the field of cybercrime investigations.

B. Drawbacks of Existing System:

It is true that selecting a consensus method, like Proof of Work or Proof of Stake, can affect how cybercrime cases are investigated. When it comes to Proof of Work, the environmental issues brought on by the heavy processing load needed for mining have the potential to impede the verification and validation procedures. There are both practical and ethical reasons to be concerned about this environmental impact of Proof of Work, given its high energy consumption and carbon footprint. On the other hand, because Proof of Stake involves validators who lock up cryptocurrency holdings in order to take part in the consensus process, it may present complicated governance issues. The overall effectiveness of investigations may be impacted by these governance complications, which may also cause delays or uncertainty in the evidence verification process. Furthermore, while fuzzy hashing adds a layer of nuance, it may also introduce subjectivity in the assessment of evidence similarities. Rather than offering exact matches, fuzzy hashing uses algorithms to assess the levels of similarity between data. This subjectivity may cause arguments or disagreements about how to interpret the evidence, especially when it comes to legal proceedings.

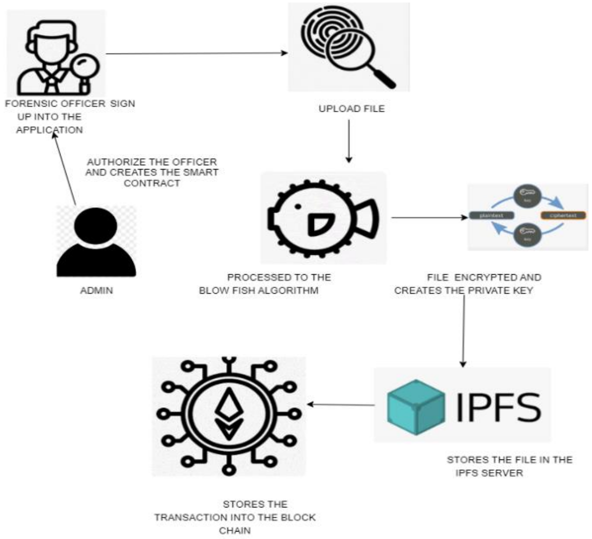
V PROPOSED SYSTEM

Preserving digital evidence is essential for linking suspects to illicit activity in cybercrime investigations. Blockchain offers tamper-resistance, but its vulnerability is that data is left exposed due to the lack of encryption. The proposal combines the BLOWFISH encryption algorithm with Solidity for smart contracts to strengthen security. Evidence files are encrypted by BLOWFISH before being stored in the blockchain, making data unreadable in the absence of the decryption key. The risk of illegal access or tampering is greatly decreased by this extra security layer, protecting the confidentiality and integrity of the evidence. This methodology guarantees a stronger basis for judicial proceedings and preserves the confidentiality of electronic evidence in cybercrime inquiries.

A. Advantages of the proposed System

A vital layer of security is added when digital evidence encrypted before being stored in a blockchain. This ensure the integrity and confidentiality of the data by making it unreadable without the decryption key. The encryption serves as a barrier, preventing access to sensitive data even in the event that unauthorized access to the blockchain occurs. The robustness of encryption and blockchain's resistance to tampering together provide strong defense 3 against data manipulation, making it extremely difficult for bad actors to falsify evidence. This method greatly helps cybercrime investigations and legal proceedings by strengthening the blockchain's dependability as a secure repository and enhancing the credibility of digital evidence.

B. Block Diagram


FORENSIC OFFICER SIGN UP INTO THE APPLICATION
UPLOAD FILE
AUTHORIZE THE OFFICER AND CREATES THE SMART CONTRACT
ADMIN
PROCESSED TO THE BLOW FISH ALGORITHM
key
plaintext
ciphertext
key
FILE ENCRYPTED AND CREATES THE PRIVATE KEY
IPFS
STORES THE FILE IN THE IPFS SERVER
STORES THE TRANSACTION INTO THE BLOCK CHAIN

C. Modules Description

1.**CREATING SMART CONTRACT FOR THE OFFICER**: Using blockchain technology, forensic investigators can create a safe, automated system for officer logins by creating a smart contract. Officer access to confidential forensic data would be managed and authenticated by the smart contract. It might have features like access control systems, unique identification protocols, and biometric verification. Every interaction would be logged by this contract, giving an unchangeable and transparent record of each officer's login activities and the tasks they completed inside the forensic system. By putting in place a smart contract of this kind, the system supports the integrity of forensic processes by guaranteeing increased security, accountability, and transparency in controlling officer access to vital investigative data.

2.**DATA ENCRYPTION MODULE (BLOW FISH ENCRYPTION):** The Data Encryption Module uses Blowfish encryption, a reliable technique that converts data into unintelligible ciphertext to guarantee data confidentiality. The data cannot be reversed into a readable format without the decryption key. This strong encryption protects the confidentiality of data within the block chain by preventing unwanted access. The Block chain Storage Module securely stores encrypted data, thwarting tampering and unauthorized access by utilizing the decentralized and immutable nature of the block chain. In doing so, the block chain creates a secure environment for sensitive data by guaranteeing data integrity, traceability, and reliability.

3. **ACCESS CONTROL MODULE**: The core component of system security is the Access Control Module, which controls user permissions to regulate interactions with stored data. It serves as a gatekeeper by defining and enforcing authorized access, controlling user behavior to stop illegal entry and possible security breaches. This module reduces the possibility of data manipulation or illegal access, which is essential for protecting private data and preserving the accuracy of digital evidence. It is an essential part of systems devoted to data security and digital forensics, guaranteeing the reliability of stored data.

4. **STORING IN THE IPFS SERVER**: Forensic investigations may benefit from the use of IPFS (InterPlanetary File System) servers for data storage. IPFS provides distributed and decentralized file storage with high resilience and accessibility. Using an IPFS server in forensic settings makes it possible to store digital evidence in an immutable and timestamped manner, facilitating the safe preservation and tracking of evidence chains. This technique offers a reliable and effective way to store and retrieve evidence while maintaining its integrity during the course of an investigation

5. **STORES THE TRANSACTION IN THE BLOCK CHAIN**: Using blockchain technology and a proof-of-stake (PoS) algorithm offers forensic contexts a safe way to keep track of transaction histories. In contrast to proof-of-work, proof

IV RESULTS AND DISCUSSION

The integration of blockchain technology into forensic investigations marks a groundbreaking advancement in the field of digital forensics and evidence management. Forensic investigations play a pivotal role in upholding justice, and the proposed system takes a significant leap forward by introducing a secure and technologically advanced approach. The immutability and decentralization inherent in blockchain technology provide an unassailable fortress for forensic evidence, safeguarding it from tampering and unauthorized access. Moreover, smart contracts automate critical tasks, reducing the potential for human error and expediting the investigation process. In an era where the volume and complexity of digital evidence continue to grow, this integration proves indispensable for forensic professionals, legal practitioners, and the criminal justice system as a whole. It offers a future where forensic investigations are conducted with the utmost security, efficiency, and integrity, ultimately ensuring that the pursuit of justice remains unwavering in the face of evolving challenges.

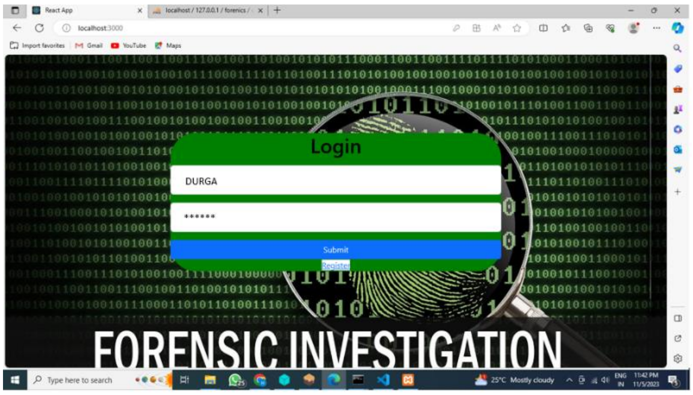


Fig 1: Office Registration

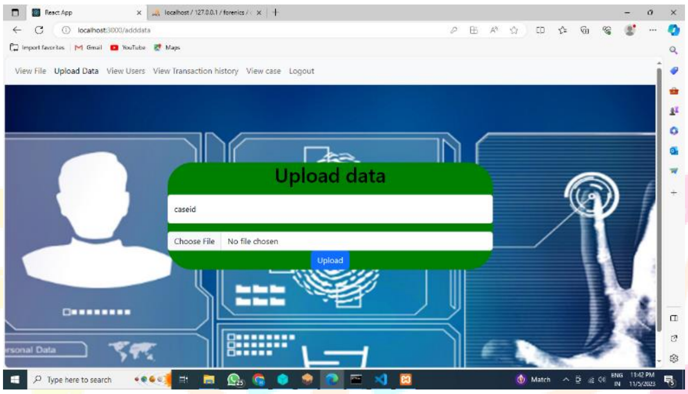
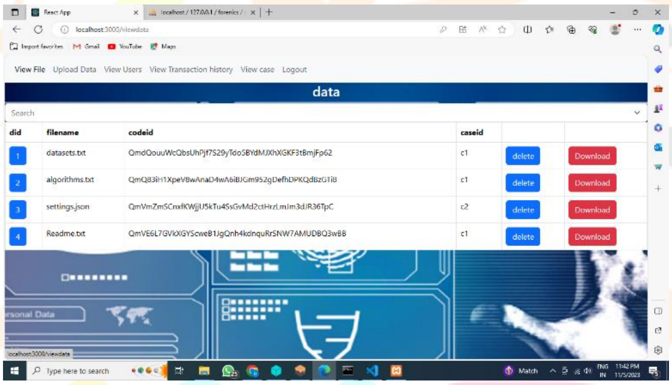
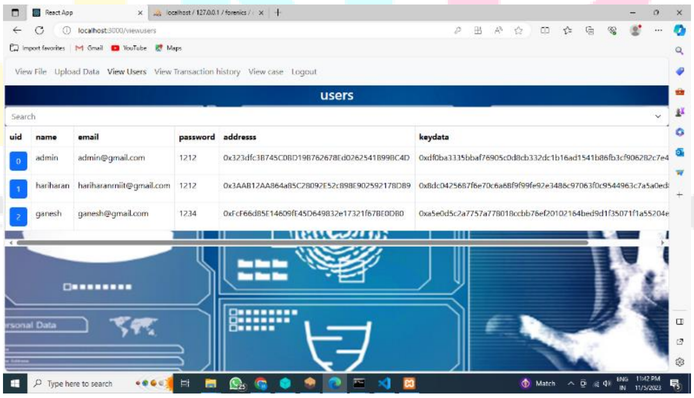

React App
localhost:3000/adddata
View File Upload Data View Users View Transaction history View case Logout
Upload data
caseid
Choose File No file chosen
Upload

Fig 2: Upload Data


React App
localhost:3000/viewdata
View File Upload Data View Users View Transaction history View case Logout
data
Search

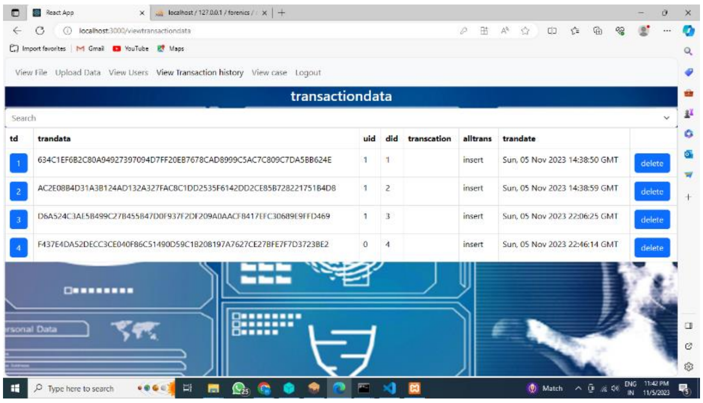
did	filename	codeid	caseid		
1	datasets.txt	QmdQouuWcQbsUhPjf7S29yTdo5BYdMJXhXGKF3tBmjFp62	c1	delete	Download
2	algorithms.txt	QmQ83iH1XpeVBwAnaD4wA6iBJGm952gDefhDPKQdBzGTiB	c1	delete	Download
3	settings.json	QmVmZmSCnxfKWjjU5kTu4SsGvMd2ctHrzLmJm3dJR36TpC	c2	delete	Download
4	Readme.txt	QmVE6L7GVkXGYScweB1JgQnh4kdnquRrSNW7AMUDBQ3wBB	c1	delete	Download

Fig 3: Stores in the IPFS Server


React App
localhost:3000/viewusers
View File Upload Data View Users View Transaction history View case Logout
users
Search

uid	name	email	password	addresss	keydata
0	admin	admin@gmail.com	1212	0x323dfc3B745C0BD19B762678Ed0262541B99BC4D	0xdf0ba3335bbaf76905c0d8cb332dc1b16ad1541b86fb3cf906282c7e4
1	hariharan	hariharanmiit@gmail.com	1212	0x3AAB12AA864a85C28092E52c898E902592178D89	0x8dc0425687f6e70c6a68f9f99fe92e3486c97063f0c9544963c7a5a0ed
2	ganesh	ganesh@gmail.com	1234	0xFcF66d85E14609fE45D649832e17321f67BE0DB0	0xa5e0d5c2a7757a778018ccbb76ef20102164bed9d1f35071f1a55204e

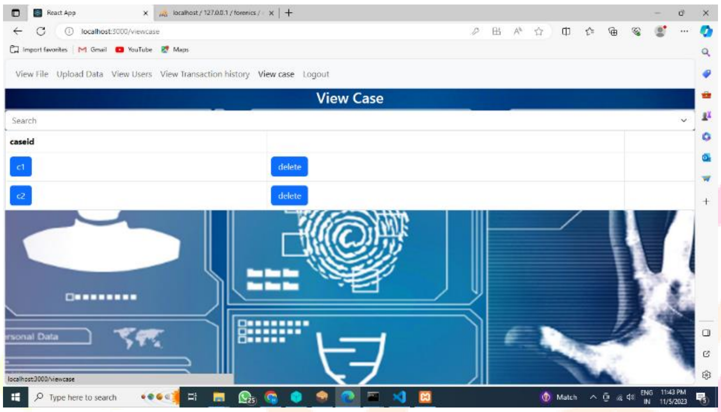
Fig 4: ID created



transactiondata

td	trandata	uid	did	transcation	alltrans	trandate	
1	634C1EF6B2C80A94927397094D7FF20EB7678CAD8999C5AC7C809C7DA5BB624E	1	1		insert	Sun, 05 Nov 2023 14:38:50 GMT	delete
2	AC2E08B4D31A3B124AD132A327FAC8C1DD2535F6142DD2CE85B728221751B4D8	1	2		insert	Sun, 05 Nov 2023 14:38:59 GMT	delete
3	D6A524C3AE5B499C27B455B47D0F937F2DF209A0AACFB417EFC30689E9FFD469	1	3		insert	Sun, 05 Nov 2023 22:06:25 GMT	delete
4	F437E4DA52DECC3CE040F86C51490D59C1B208197A7627CE27BFE7F7D3723BE2	0	4		insert	Sun, 05 Nov 2023 22:46:14 GMT	delete

Fig 5: Transaction stores in the Ganache



View Case

caseid	
c1	delete
c2	delete

Fig 6: Delete File

Acknowledgment

The preferred spelling of the word "acknowledgment" in an Indian authors , Title and content is very clear about Forensics Evidence project. It is Copyright content.."thanks".

References

[1] Li, S.; Qin, T.; Min, G. Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Trans. Compute Soc. Syst. 2019, 6, 1433–1441. [CrossRef]

[2] Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 4177–4186. [CrossRef]

[5] Truex, S.; Baracaldo, N.; Anwar, A.; Steinke, T.; Ludwig, H.; Zhang, R.; Zhou, Y. A Hybrid Approach to Privacy-Preserving Federated Learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, London, UK, 15 November 2019; pp. 1–11. [CrossRef]

[6] Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated Learning. 2020. Available online: https://link.springer.com/book/10.1007/978-3-031-01585-4