DIGITAL EVIDENCE MANAGEMENT USING BLOCKCHAIN

4 authors:

Namitha Cv
Sree Narayana Gurukulam College of Engineering
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Revathy Salimon
Sree Narayana Gurukulam College of Engineering
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Priya Thampi
Sree Narayana Gurukulam College of Engineering
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Nimisha .J
Sree Narayana Gurukulam College of Engineering
1 PUBLICATION **0** CITATIONS
SEE PROFILE

DIGITAL EVIDENCE MANAGEMENT USING BLOCKCHAIN

Namitha CV
Dept. Computer Science And Engineering
Sree Narayana Gurukulam College of Engineering
Kochi, Kerala
namithacv5@gmail.com

Priya Thampi
Dept. Computer Science And Engineering
Sree Narayana Gurukulam College of Engineering
Kochi, Kerala
priyathampi777@gmail.com

Nimisha J
Dept. Computer Science And Engineering
Sree Narayana Gurukulam College of Engineering
Kochi, Kerala
nimishaj2002@gmail.com

Revathy Salimon
Dept. Computer Science And Engineering
Sree Narayana Gurukulam College of Engineering
Kochi, Kerala
revathysalimon@gmail.com

Abstract—

Here we propose a pioneering two-level blockchain system for evidence management, incorporating advanced security features through the integration of cryptographic keys. The first tier entails the implementation of a public blockchain, serving as a decentralized ledger to document crucial evidence-related information, such as chain of custody, metadata, and timestamps. This ensures transparency, tamper resistance, and immutability of the recorded data. Concurrently, a private blockchain operates in tandem, exclusively accessible to authorized stakeholders, including law enforcement agencies and legal entities. Employing a permission framework, the private blockchain enhances security by controlling access to sensitive data. The second facet of the proposed system introduces cryptographic keys to fortify overall security. Each authorized entity within the private blockchain is assigned a unique cryptography key pair, comprising a public key for identification and a private key for secure access. Asymmetric cryptography guarantees that only entities possessing the corresponding private key can access or modify information within the private blockchain, providing an additional layer of protection. Furthermore, cryptographic hashing techniques generate unique fingerprints for each piece of evidence, serving as digital signatures for verification purposes.This comprehensive approach, combining the benefits of a decentralized public blockchain with controlled access and heightened security features of a private blockchain, aims to revolutionize evidence management by addressing challenges related to transparency, security, and integrity within the legal law enforcement domains.

Index Terms— Existing System; Proposed System;Security;

I.INTRODUCTION

The security of computer network infrastructure in companies, organizations, and governments has a unique role in maintaining the sustainability of information systems from cyber-attacks and minimizing loss . Digital evidence management is a crucial

the sustainability of information systems from cyber-attacks and minimizing loss . Digital evidence management is a crucial

aspect of modern investigative and legal processes, especially in the context of law enforcement, legal proceedings, and cybersecurity. It involves the collection, storage, analysis, and presentation of digital evidence in a way that ensures its integrity, authenticity, and admissibility in a court of law.

One application of computer network security systems using sniffing or monitoring techniques allows administrators to monitor the data traffic and all activities and save the network monitoring results into a log file. Generally, investigators will secure and manage those results to a centralized local device after discovering digital evidence of a cyberattack because it is temporary. However, digital evidence security systems are often overlooked and have the possibility of vulnerabilities so that attackers can exploit the system to modify and even delete data . Some of the solutions in the previous research,namly proposing a security framework using blockchain with a cluster structure,multi signature mechanisms. The study entitled digital forensic approaches for the Amazon Alexa ecosystem proposes a new approach in cloud-native forensics with client-side forensics in support of practical investigations and using cloud-based digital evidence storage . Based on this, the next challenge is obtaining, managing, and ensuring digital evidence storage . This study aims to overcome the problem of security and management of digital evidence storage. Blockchain technology has emerged as a potential solution to enhance the trustworthiness and security of digital evidence management systems. Blockchain is a decentralized and distributed ledger that records transactions across a network of computers in a secure and transparent manner. It operates on a consensus mechanism, making it resistant to tampering and providing a verifiable and immutable record of events

II.LITERATURE REVIEW

[1].**An Implementation of Blockchain Technology in Forensic Evidence Management**:-The implementation of blockchain technology in forensic evidence management i nvolves a systematic approach to secure, transparent, and immutable storage of digital evidence. The methodology typically begins with the creation of a decentralized and distributed ledger using blockchain, where each piece of forensic evidence is assigned a unique cryptographic hash and recorded as a transaction. This ledger is maintained by a network of nodes, ensuring that no single entity has control over the entire system. The use of smart contracts can automate the validation and verification of evidence, enhancing the integrity and efficiency of the forensic process. Additionally, the implementation may involve the integration of cryptographic techniques to secure the privacy and confidentiality of sensitive information within the blockchain it enhanced transparency and traceability, reducing the risk of tampering or corruption of crucial evidence also such as the potential scalability issues with certain blockchain networks and the need for careful consideration of legal and regulatory frameworks to ensure compatibility with existing forensic procedures.

[2]. **An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash":-** The enhanced blockchain-based IoT digital forensics architecture integrates IoT devices and sensors, employing fuzzy hash functions to hash digital evidence resiliently to minor data changes. These hashed values are securely stored on a blockchain, ensuring immutability and traceability. Smart contracts automate validation, and verification processes, streamlining the workflow. This architecture enhances tamper resistance and integrity verification in IoT digital forensics, addressing challenges posed by dynamic data. The decentralized nature of the blockchain provides a secure, auditable evidence trail, though potential implementation complexities, scalability concerns, and resource requirements should be carefully considered during adoption**.**

[3]. **IoT Forensics System based on Blockchain":-**

The IoT Forensics System based on Blockchain integrates IoT devices with a blockchain framework to enhance digital forensics. The methodology involves collecting and timestamping digital evidence from IoT devices, creating an immutable ledger on the blockchain. This decentralized ledger ensures data integrity, and smart contracts automate verification processes, contributing to security and transparency in forensic investigations. The system provides advantages such as tamper-resistant digital evidence and improved traceability. However, potential drawbacks include scalability challenges and the need for careful consideration of adoption costs and user training, as blockchain technology may require a learning curve for forensic investigators and initial resource investments.

[4]. **An Implementation of Blockchain Technology in Combination with IPFS for Crime Evidence Management System:-** The implementation of blockchain technology alongside IPFS for a Crime Evidence Management System involves creating a tamper-resistant ledger on the blockchain to record and timestamp crime evidence, with each piece of evidence linked to the IPFS network for decentralized file storage. This integrated methodology ensures data integrity, accessibility, and transparency in evidence management. Advantages include heightened security and immutability of evidence through blockchain, while IPFS contributes to efficient decentralized file storage. However, potential challenges encompass scalability concerns, particularly with a high volume of evidence files, and the necessity for careful consideration of implementation costs and adherence to legal frameworks for seamless integration into crime evidence management systems.

[5]. **Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer Digit**:- The Forensic-chain paper outlines a methodology for developing a secure and transparent digital forensics chain of custody using blockchain technology, with a Proof of Concept (PoC) implemented in Hyperledger Composer. The process involves creating a decentralized and immutable ledger, uniquely identifying each forensic artifact and recording transactions on the blockchain to ensure tamper-resistant and auditable chain of custody. Advantages of the system include heightened security and transparency, facilitated by blockchain's decentralized nature, and the tailored capabilities of Hyperledger Composer for forensic applications. However, potential challenges include the need for specialized knowledge in Hyperledger Composer, scalability concerns, and considerations for interoperability with existing forensic tools. Attentiveness to these factors is crucial for the successful adoption and integration of the proposed digital forensics chain of custody system.

[6]. **Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric:-** The paper on the "Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric" presents a methodology focused on establishing a robust digital evidence management system using Hyperledger Fabric. The process involves creating a permissioned blockchain network where digital evidence is securely stored, timestamped, and linked to unique cryptographic identifiers. Smart contracts are utilized for automating evidence management tasks, ensuring transparency and accountability. The model leverages the privacy and permission features of Hyperledger Fabric, allowing designated entities to access and manage evidence based on predefined roles. The advantages of this approach include enhanced security immutability, and controlled access to digital evidence, as well as the scalability and efficiency offered by Hyperledger Fabric. However, potential disadvantages may include the need for specialized knowledge in blockchain and Hyperledger

Fabric, and careful consideration of the associated implementation and maintenance costs, which are essential factors for successful adoption in digital evidence management systems.

[7]. **A Study on a Model Frame for the Integration of Digital Forensic Processes; Korean Institute of Criminology:-**

Likely employs a methodology that encompasses a comprehensive analysis of existing digital forensic processes, standards, and technologies. The aim may be to identify commonalities and overlaps in the various stages of digital forensics, proposing a unified model that optimizes efficiency and collaboration among forensic practitioners. The study may involve the development and testing of prototypes or simulations to validate the proposed integration model. The advantages of such an integrated framework lie in its potential to enhance the effectiveness of digital forensic investigations by providing a standardized approach, reducing redundancy, and facilitating seamless information sharing among investigators. However, potential challenges may include the need for widespread adoption and acceptance of the proposed model within the digital forensic community, as well as addressing the dynamic nature of technology and emerging forensic methodologies. These considerations are crucial for ensuring the successful implementation and long-term viability of the integrated digital forensic processes model.

[8]. **Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment:-**

This hierarchical structure ensures efficient scalability and management of IoT networks. The methodology involves implementing interoperability protocols, appropriate consensus mechanisms, and integrating smart contracts with oracles. This approach enhances scalability by distributing tasks across layers, optimizing resource utilization, and facilitating seamless communication between devices. The advantages include improved scalability, tailored consensus mechanisms for efficiency, and the automated execution of smart contracts, creating a robust and scalable environment for IoT applications. However, challenges may arise in terms of complexity and potential centralization in the top-tier blockchain, requiring careful consideration during implementation.

[9]. **Robust and secure evidence management in digital forensics investigations using blockchain technology:-**

In establishing robust and secure evidence management for digital forensics investigations, blockchain technology serves as a promising solution. The methodology involves the creation of a decentralized and tamper-resistant ledger to record and authenticate digital forensic evidence. Each piece of evidence is timestamped and linked cryptographically, ensuring its integrity throughout the investigation. The blockchain's consensus mechanism enhances trust by preventing unauthorized alterations to the stored data. Advantages of this approach include increased transparency, immutability, and the ability to trace the chain of custody seamlessly. Furthermore, it mitigates the risk of data manipulation and enhances the overall security of digital forensic processes. However, challenges may arise in terms of scalability, as storing large volumes of forensic data on a blockchain could lead to performance issues. Additionally, the integration of blockchain technology requires addressing legal and regulatory considerations to ensure its admissibility in court. Despite these challenges, the methodology provides a robust foundation for secure evidence management in digital forensics investigations.

[10]. **Joining Federated Learning to Blockchain for Digital Forensics in IoT:-** Joining Federated Learning to Blockchain for Digital Forensics in IoT involves a synergistic approach to enhance the security and efficiency of forensic investigations. The methodology integrates federated learning, enabling model training across decentralized IoT devices without sharing raw data, with a blockchain-based infrastructure to ensure tamper-proof evidence management. Federated learning allows collaborative model training while preserving individual privacy, and the blockchain guarantees the integrity and transparency of forensic data. Advantages include enhanced privacy protection, improved accuracy in forensic analyses through collaborative learning, and a secure, decentralized evidence trail stored on the blockchain. However, challenges may arise in terms of computational overhead associated with federated learning and potential scalability issues with blockchain integration. Striking a balance between these technologies and addressing interoperability concerns is crucial for successful implementation in the context of digital forensics in the IoT.

[11]. **The Oracle Paradox of Blockchain Smart Contracts.:-** The Oracle Paradox in Blockchain Smart Contracts refers to the challenge of securely incorporating real-world data into decentralized applications. The methodology involves using oracles, which are third-party services that fetch and provide external data to smart contracts. Advantages of oracles include expanding the functionality of smart contracts by allowing them to interact with real-world data, enabling applications like decentralized finance (DeFi). However, disadvantages include the potential for oracles to become central points of failure or manipulation, compromising the trustless nature of blockchain. Security risks arise if the data source is compromised or if the oracle is malicious, leading to incorrect execution of smart contracts. Striking a balance between functionality and security is crucial in navigating the Oracle Paradox in Blockchain Smart Contracts.

III.EXISTING SYSTEM

Existing system refers to the conventional methods and technologies currently utilized for managing forensic evidence in criminal investigations. The existing system typically involves a combination of manual processes, paper- based documentation, and centralized databases. The methodology for the proposed two-level blockchain for evidence management with enhanced security using cryptographic keys is designed to create a comprehensive and secure framework for handling sensitive information within the legal and law enforcement sectors. The first step involves the establishment of a two-tiered blockchain architecture. In the first level, a public blockchain is implemented to record high-level information related to evidence, such as the chain of custody, metadata, and timestamps. This public blockchain is decentralized, ensuring that information is transparent, tamper-resistant, and immutable. Simultaneously, the second level employs a private blockchain that operates alongside the public blockchain and is accessible only to authorized stakeholders. This evidence

private blockchain serves as a repository for sensitive data, utilizing a permissioned framework to control access. This bifurcated approach addresses the need for transparency in evidence management while simultaneously safeguarding critical information through controlled access. The second phase of the methodology involves the integration of cryptographic keys to enhance security. Each authorized entity within the private blockchain is assigned a unique cryptographic key pair – a public key for identification and a private key for secure access. Asymmetric cryptography is employed, ensuring that only entities possessing the corresponding private key can access or modify information
within the private blockchain. This cryptographic key infrastructure adds a layer of protection against unauthorized access, ensuring the confidentiality and integrity of sensitive data. Additionally, cryptographic hashing techniques are applied to generate unique fingerprints for each piece of evidence. These cryptographic hashes act as digital signatures, enabling stakeholders to verify the authenticity of without compromising the security of the underlying information.
The third step in the methodology focuses on the decentralized verification layer provided by the public blockchain. Authorized users can cross-reference cryptographic hashes stored in the public blockchain to verify the integrity of evidence without direct access to sensitive information in the private blockchain. This decentralized verification mechanism ensures that the information stored in the private blockchain remains secure while allowing for transparent and accountable evidence management through the public blockchain.

Disadvantages:

- Less reliability and secure
- Data leakage
- Downtime and Service Reliability
- Concerns About Long-Term Viability

IV.PROPOSED SYSTEM

The proposed two-level blockchain for evidence management with enhanced security using cryptographic keys represents an innovative approach to address the complexities and security concerns inherent in traditional evidence management systems. The first methodology involves the establishment of a two-tiered blockchain architecture. The first level, often referred to as the public blockchain, is responsible for recording and validating high-level information related to the evidence. This includes the creation of a decentralized ledger that records the chain of custody, metadata, and timestamps associated with each piece of evidence. The decentralized nature of this level ensures transparency and immutability, making it resistant to tampering or unauthorized alterations. Simultaneously, the second level, or private blockchain, operates alongside the public blockchain and is accessible only to authorized stakeholders such as law enforcement agencies, forensic experts, and legal entities. This private blockchain stores sensitive information, utilizing a permissioned framework to control access, thus adding an extra layer of security to critical data.

The second methodology involves the integration of cryptographic keys to enhance the overall security of the evidence management system. Each authorized entity within the private blockchain is assigned a unique cryptographic key pair—a public key for identification and a private key for secure access. The use of asymmetric cryptography ensures that information can only be accessed or modified by entities possessing the corresponding private key, thereby preventing unauthorized tampering or data breaches. Additionally, cryptographic hashing techniques can be employed to generate unique fingerprints for each piece of evidence, enhancing data integrity. The public blockchain, in this context, acts as a decentralized verification layer, allowing stakeholders to cross-reference the cryptographic hashes and verify the authenticity of evidence without compromising sensitive information stored in the private blockchain.

The proposed two-level blockchain evidence management system offers several advantages. Firstly, it provides a transparent and immutable record of evidence through the public blockchain, ensuring accountability and trust in the chain of custody. Secondly, the private blockchain enhances security by restricting access to sensitive data, safeguarding the integrity of evidence-related information. Thirdly, the use of cryptographic keys adds an additional layer of protection, securing access to information and preventing unauthorized manipulation. Moreover, the decentralized and distributed nature of the system minimizes the risk of a single point of failure, further fortifying the resilience and reliability of the evidence management framework.

In conclusion, the proposed two-level blockchain for evidence management, coupled with enhanced security using cryptographic keys, presents a comprehensive and robust solution to the challenges faced by traditional systems. By leveraging a decentralized architecture, permissioned access, and cryptographic techniques, this system aims to revolutionize evidence management, ensuring transparency, security, and integrity in the handling of critical information within the legal and law enforcement domains.

Advantages:

- Decentralization.
- Reduced Single-Point-of-Failure.
- Token-Based System.
- Elimination of Intermediaries.
- Collective Decision-Making.
- Optimized Resource Utilization.

V.SYSTEM ARCHITECTURE

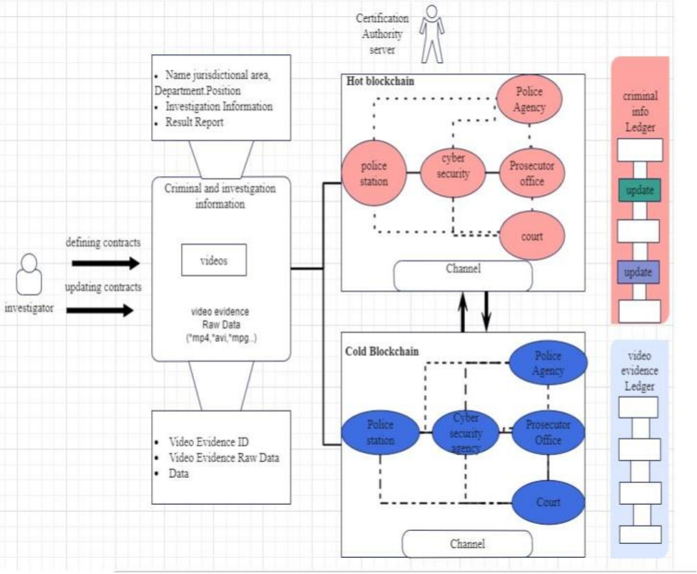


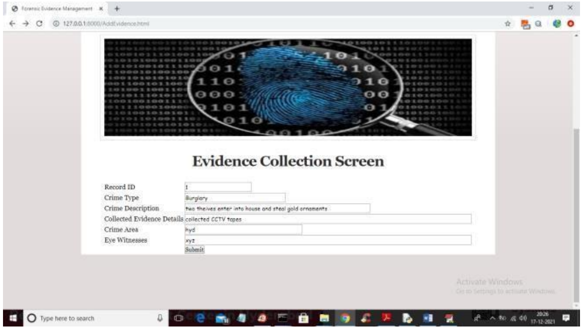
Fig 1: - System Architecture.

Our envisioned two-tier blockchain system for the streamlined management of crime evidence incorporates two layers, overseen by hot and cold blockchains. The hot blockchain is designated for storing investigation and identity information characterized by frequent transaction fluctuations throughout the criminal investigation process. On the other hand, the cold blockchain is dedicated to housing digital crime evidence videos that demand unaltered storage without subsequent modifications.

Institutions corresponding to the national police agency, local police agency, cyber analysis team, prosecutor's office, and courts—which are the peers in the channel—would form a consortium in order to participate in blockchain channels and share the identity and investigation information in the hot blockchain using the process. When registering an identity, the authentication server issues a private key belonging to the national police agency peer to the on-site investigator. the on-site investigator obtains the authority to access the hot blockchain through the issued private key, and can store the investigation and identity information. Users who do not have keys belonging to the national police agency peer cannot access or store data on a hot blockchain. The transactions delivered by the on-site investigator to the hot blockchain include ID, name, social security number, department, jurisdiction, date, investigation information, and evidence ID. In addition, only investigators with verified identities and those in the judicial system can transfer transactions to the chaincode. After the transaction has been delivered, a block containing the identity and investigation information is created through the chaincode, which is a predefined smart contract source code, and the transaction and block are distributed to all organizations participating in the blockchain.

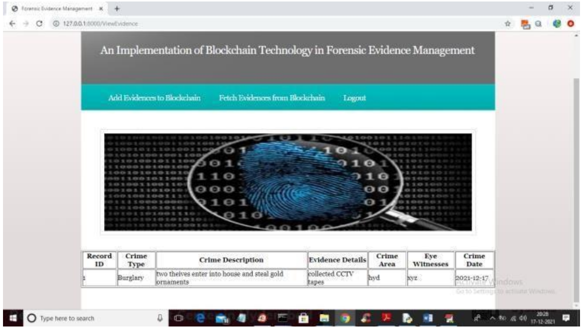
VI.RESULTS

Officers or administrators can send in the report after filling out the preceding page by clicking on the "Submit" button.



Evidence Collection Screen

Record ID	1
Crime Type	Burglary
Crime Description	two theives enter into house and steal gold ornaments
Collected Evidence Details	collected CCTV tapes
Crime Area	hyd
Eye Witnesses	xyz



127.0.0.1:8000/ViewEvidence

An Implementation of Blockchain Technology in Forensic Evidence Management

Record ID	Crime Type	Crime Description	Evidence Details	Crime Area	Eye Witnesses	Crime Date
1	Burglary	two theives enter into house and steal gold ornaments	collected CCTV tapes	hyd	xyz	2021-12-17

This report articulates a comprehensive vision for our proposed TwoLevel Blockchain system, poised to revolutionize the landscape of crime evidence management. The intricate design integrates two distinct layers, each governed by hot and cold blockchains, embodying a sophisticated framework tailored to the evolving demands of criminal investigations.The hot blockchain emerges as a dynamic repository, strategically engineered to adeptly handle investigation and identity information. It provides a resilient latform capable of accommodating the continuous flux of transactions inherent in the intricate and multifaceted criminal investigation process. This layer ensures the real-time and secure storage of crucial data, fostering a responsive and adaptable environment in the face of the dynamic nature of investigative proceedings. In tandem, the cold blockchain assumes its role as the custodian of digital crime evidence videos, offering a stable and unyielding sanctuary for materials that necessitate unaltered preservation post-storage. The cold blockchain, characterized by its immutability and steadfast nature, serves as the bedrock for ensuring the integrity and authenticity of digital evidence, crucial in legal proceedings.This pioneering approach, harnessing the dual strengths of both hot and cold blockchains, signifies a quantum leap in the paradigm of evidence management. It not only acknowledges but addresses the inherent complexities and diverse requirements of modern criminal investigations. By amalgamating the agility of the hot blockchain with the steadfast assurance of the cold blockchain, our proposed system stands as a testament to innovation and foresight in the realm of forensic technology.As we transition into subsequent phases, the focus will shift towards the meticulous implementation of this conceptual framework. Harnessing the insights gleaned from this initial phase, we are poised to refine and actualize the Two-Level Blockchain system, ensuring its alignment with the highest standards of security, efficiency, and adaptability. The iterative nature of our development process allows for continuous enhancements and adaptations, underscoring our commitment to delivering a robust and resilient evidence management platform that transcends contemporary limitations.

IX. FUTURE ENHANCEMENT

In the realm of digital evidence management, blockchain technology holds significant promise for future enhancements, particularly in ensuring the integrity and security of evidentiary data. One key advantage lies in the immutable nature of blockchain, where once digital evidence is recorded, it becomes resistant to tampering or unauthorized alterations. This feature ensures a transparent and unchangeable record of the evidence's lifecycle, thereby reinforcing the chain of custody and bolstering the credibility of the evidence in legal proceedings. Moreover, the adoption of decentralized storage systems, facilitated by blockchain, can distribute digital evidence across a network of nodes. This decentralization not only enhances the security of the stored information but also mitigates the risks associated with data loss or tampering by maintaining multiple copies of the evidence across the network. Additionally, the implementation of smart contracts within blockchain frameworks can automate and enforce predefined rules and conditions, streamlining processes such as evidence collection, authentication, and access, while minimizing the potential for human error or manipulation. These advancements collectively contribute to a more robust, transparent, and secure digital evidence management system, aligning with the evolving needs of modern investigative and legal practices.

X. REFERENCE

[1]. An Implementation of Blockchain Technology in Forensic Evidence Management by **R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip and N. Singh.** March 2021. DOI:10.1109/ICCIKE51210.2021.9410791

[2.]An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash by **W. A. Mahrous, M. Farouk and S. M. Darwish.** 2021.DOI: 10.1109/ACCESS.2021.312671
IoT Forensics System based on Blockchain by **Y. Makadiya, R. Virparia and K. Shah** 2023

[3].An Implementation of Blockchain Technology in Combination with IPF Crime Evidence Management System **C. Shilpa and A. H. Shanthakumar .**

[4]. Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer Digit by **LoneA.H** 2019

[5].Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems2023, Internet of Things (Netherlands).

[6.] A Study on a Model Frame for the Integration of Digital Forensic Processes; Korean Institute of Criminology by **Tak, H.S.; Lee, W.S,2016**
[7]Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment

[8]. Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment by **Oktian, Y.E; Lee, H.J,2020.**

[9] Robust and secure evidence management in digital forensics investigations using blockchain technology 2023.

[10] Joining Federated Learning to Blockchain for Digital Forensics in IoT 2023.

[11]The Oracle Paradox of Blockchain Smart Contracts **Albizri, A.; Appelbaum, D** 2021.