IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 14, Issue 4, April 2024, ||Series -2|| PP 141-149

Implementing a Blockchain- Based Evidence Protection System

[1] **V. Jyothi sri,** *B.Tech Student, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, vurajyothisri@gmail.com*

[2] **Ch. Siddhartha**, *B.Tech Student, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, chanapathisiddhartha@gmail.com*

[3] *T*. **Malleswararao**, *B.Tech student, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, tirumanimalleswararao@gmail.com*

[4] **A. Revathi**, *B.Tech student, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY, andanalapallirevathi@gmail.com*

[5] **Mr. K. Surya Ram Prasad**, *M. Tech, Assistant Professor, Department of CSE, DNR College of Engineering and Technology, surya.dnrcet@gmail.com*

Abstract: *This paper presents an innovative solution, the Implementing a Blockchain-Based Evidence Protection system, designed to address critical challenges in contemporary legal and investigative practices. Leveraging blockchain technology, specifically Ethereum, the EPS ensures the integrity, authenticity, and security of evidence throughout its lifecycle. By employing cryptographic methods, timestamps, and smart contracts, the system establishes a tamper-proof, transparent, and decentralized platform for evidence management. Through digital timestamps and distributed ledger technology, the EPS creates an immutable record of evidence, eliminating vulnerabilities associated with centralized systems. Smart contracts automate processes such as access control and chain of custody, enhancing security and transparency. Encryption and hashing techniques safeguard sensitive information while enabling verification of integrity. Overall, the System offers a comprehensive solution to the complexities of evidence management in modern legal environments, providing confidence in the reliability and trustworthiness of stored evidence.*
Index Terms: Evidence Protection, Blockchain, Ganache, Metamask, SHA-256

I. INTRODUCTION

In contemporary legal and investigative landscapes, the management and protection of evidence stand as paramount pillars of the justice system. Ensuring the integrity, authenticity, and security of evidence is not only essential during the investigation phase but also crucial in maintaining the trust and reliability of the legal process [1]. However, traditional methods of evidence management have faced significant challenges, ranging from vulnerabilities to tampering, unauthorized access, and a lack of transparency [2].

Conventional approaches to evidence management often relied on centralized databases or physical documentation, which inherently carried vulnerabilities such as data tampering and unauthorized alterations due to the absence of robust verification mechanisms [3]. These weaknesses underscored the urgent need for a more secure and tamper-proof solution that could safeguard sensitive information effectively [4].

To address these challenges, this paper proposes the Implementing a Blockchain-Based Evidence Protection system that leverages blockchain technology. The integration of blockchain aims to enhance the security, reliability, and transparency of managing evidence across various domains, including legal, financial, and sensitive data management [5].

The System seeks to establish a robust system for protecting evidence by harnessing the decentralized structure of blockchain technology. By incorporating cryptographic methods, timestamps, and smart contracts, the system aims to create a platform that ensures evidence remains tamper-proof, transparent, and authentic throughout its lifecycle [6]. This approach not only safeguards the integrity of stored evidence but also enhances the overall trustworthiness of the legal process [7].

In selecting a suitable blockchain platform for the System, Ethereum emerges as a prominent choice due to its robust features and active developer community. Ethereum's support for smart contracts, decentralized applications (DApps), security enhancements, and compatibility with various blockchain projects makes it well-suited for building and enhancing the proposed Implementing a Blockchain-Based Evidence Protection system[8].

The existing systems for evidence management and protection in legal and investigative processes face several significant challenges. Traditional methods often rely on centralized databases, which can be vulnerable to tampering and manipulation. Unauthorized access and alterations compromise the integrity of evidence, raising doubts about its reliability in legal proceedings [9].

Moreover, the lack of transparency in existing systems can lead to questions regarding the authenticity and origin of evidence, further undermining trust in the legal process [10]. Manual processes for establishing and maintaining the chain of custody are often time-consuming, error-prone, and lack real-time tracking capabilities [11]. Many existing systems also struggle to adapt to evolving technologies, posing challenges in meeting the changing demands of the legal landscape [12].

In response to these challenges, the proposed Implementing a Blockchain-Based Evidence Protection System seeks to elevate the standards of safeguarding evidence by leveraging blockchain technology. By harnessing the decentralized nature of blockchain, the system aims to create a tamper-proof and transparent system for managing evidence, thereby enhancing the integrity and reliability of the legal process [13].

Through the implementation of cryptographic security measures and smart contracts, the present system aims to ensure the authenticity and integrity of evidence while providing transparency for authorized access. By tapping into Ethereum's robust features, the EPS aims to leverage the capabilities of blockchain technology to address the shortcomings of existing evidence management systems [14].

In summary, the integration of blockchain technology offers promising opportunities to revolutionize evidence management and protection in legal and investigative processes. The proposed Implementing a Blockchain-Based Evidence Protection system represents a significant step towards enhancing the security, reliability, and transparency of managing evidence, thereby strengthening the foundations of the justice system [15].

II. LITERATURE SURVEY

The literature surrounding the utilization of blockchain technology in evidence management and digital forensics has seen significant growth in recent years. Various researchers have explored the potential of blockchain to address the challenges faced by traditional evidence management systems, such as tampering, lack of transparency, and vulnerabilities to unauthorized access. This literature survey aims to provide an overview of some key studies in this field, highlighting their methodologies, findings, and contributions.

Jamulkar et al. [16] propose an Evidence Management System (EMS) that integrates blockchain and distributed file systems to enhance the security and integrity of evidence. Their system employs blockchain for maintaining a tamper-proof record of evidence transactions, while distributed file systems ensure efficient storage and retrieval of digital evidence. Through experimental evaluation, the authors demonstrate the effectiveness of their approach in ensuring the authenticity and integrity of evidence in forensic investigations.

Banu et al. [17] focus on the application of blockchain technology specifically for securing forensic evidence. They highlight the importance of maintaining the chain of custody in forensic investigations and propose a blockchain-based solution to address this challenge. By leveraging the immutability and transparency of blockchain, their system aims to provide a tamper-proof and auditable record of evidence custody, thereby enhancing the trustworthiness of forensic processes.

Gopalan et al. [18] explore the use of blockchain in digital forensics, with a focus on ensuring the integrity and reliability of digital evidence. Their proposed framework incorporates blockchain for maintaining a secure and transparent chain of custody, enabling investigators to track the handling of digital evidence throughout the investigation process. Through experimental validation, the authors demonstrate the feasibility and effectiveness of their approach in enhancing the integrity of digital forensic procedures.

Lone et al. [19] present Forensic-chain, a blockchain-based digital forensics chain of custody system developed using Hyperledger Composer. Their system aims to address the challenges associated with traditional chain of custody processes by leveraging blockchain's immutable ledger for recording evidence transactions. Through a proof-of-concept implementation, the authors showcase the capabilities of their system in ensuring the integrity and transparency of digital forensic investigations.

Tian et al. [20] propose Block-DEF, a secure digital evidence framework that utilizes blockchain technology to enhance the integrity and reliability of digital evidence. Their framework incorporates cryptographic techniques and smart contracts to ensure the authenticity and tamper resistance of digital evidence. Through experimental evaluation and comparative analysis, the authors demonstrate the superiority of their approach in providing a robust and trustworthy platform for digital evidence management.

These studies collectively highlight the potential of blockchain technology to address critical challenges in evidence management and digital forensics. By leveraging blockchain's inherent properties such as immutability, transparency, and decentralization, researchers are able to develop innovative solutions that enhance the security, integrity, and reliability of evidence handling processes. However, further research is needed to explore practical implementation challenges, scalability issues, and real-world deployment considerations to fully realize the potential of blockchain in this domain.

III. METHODOLOGY

a) Proposed Work:

The proposed Implementing a Blockchain-Based Evidence Protection system using blockchain technology offers several advantages over traditional systems.

The use of blockchain technology ensures a decentralized and tamper-proof storage system. Evidence [3] is securely timestamped and stored in a distributed ledger, eliminating the risk of unauthorized access, manipulation, or tampering.

The project proposes a system that leverages blockchain's decentralized structure. It employs cryptographic methods, timestamps, and smart contracts to create a platform that ensures evidence remains tamper-proof, transparent, and authentic throughout its lifecycle. This ensures the integrity and reliability of stored evidence.

Ethereum, a prominent Blockchain [7] platform, is chosen for its robust features. The project taps into Ethereum's support for smart contracts.

b) System Architecture:

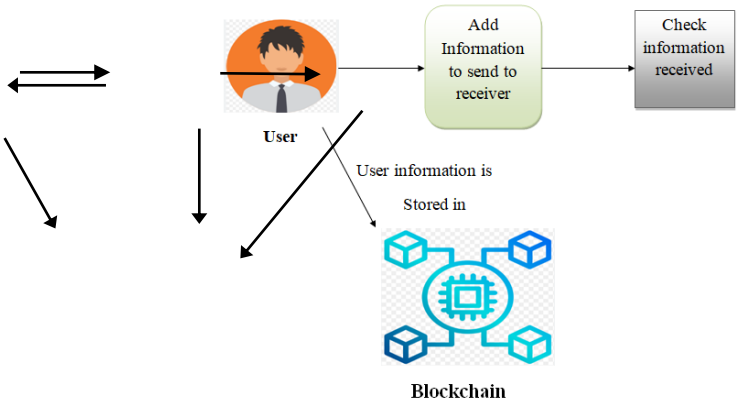

Fig1 Proposed Architecture

The system architecture comprises three main components: the User Interface, the Blockchain Network, and the Backend Server.

The User Interface facilitates interaction between the user and the system. Users input information to be sent to the receiver and verify information received. This interface ensures user-friendly communication with the system.

The Blockchain Network stores user information securely. Each user's data, including sent and received information, is stored as transactions on the blockchain. This decentralized ledger ensures immutability, transparency, and tamper-proofing of user data.

The Backend Server acts as an intermediary between the user interface and the blockchain network. It processes user requests, validates transactions, and communicates with the Blockchain [7] network. Additionally, the backend server manages user authentication and authorization processes, ensuring secure access to the blockchain.

Overall, this architecture provides a robust and secure system for sending and verifying information, leveraging blockchain technology for data integrity and transparency.

c) User Signup:

The User Signup module enables individuals to register accounts by providing personal information, credentials (username, password), and any required data. Upon successful registration, their information is securely stored within the system, possibly utilizing blockchain for data integrity. This module serves as the entry point for users to access system features and functionalities.

d) User Signin:

The User Sign-in module allows registered users to authenticate themselves using their credentials. This module verifies the provided information against stored records to grant access to the system. Upon successful authentication, users are granted access to system functionalities based on their assigned permissions and roles. This module ensures secure access to the system for authorized users, maintaining data integrity and user privacy.

1. Add information:
The Add Information module empowers users to input or upload evidence-related data into the system. This may include uploading documents, entering information, or attaching relevant files related to the managed evidence. The added information undergoes processes to ensure authenticity, immutability, and secure storage, often leveraging the capabilities of blockchain technology. This module enhances the integrity and reliability of evidence management, maintaining a transparent and tamper-proof record of information.
2. Check information:
The Check Information module enables users to access and verify data stored within the system. It offers functionalities for searching, retrieving, and viewing specific evidence or related information. This module ensures transparent access for authorized users while upholding the security and integrity of stored data. By providing users with the means to validate information, it enhances confidence in the reliability and trustworthiness of the evidence management system.
e) Blockchain Integration:
Blockchain's decentralized ledger involves storing evidence records across numerous nodes. This distribution ensures that there's no single central point of control, significantly enhancing security. Each node contains a copy of the ledger, preventing data manipulation or tampering without consensus across the network.
Within the blockchain, cryptographic hashing and timestamps are applied to evidence. This process creates a unique, irreversible digital fingerprint for each piece of evidence. Once stored, any alteration or deletion becomes computationally infeasible, establishing tamper-proof records.
Smart contracts, self-executing digital agreements, automate predefined rules and actions related to evidence management. By encoding these rules into smart contracts, the system ensures consistent execution, transparency, and reliability in managing evidence throughout its lifecycle.
Blockchain's transparent nature allows authorized users to access evidence records. This access enables verification of the evidence's authenticity and integrity. The transparent and auditable nature of blockchain fosters trust among stakeholders and ensures transparency in evidence handling.
Leveraging cryptographic techniques inherent in blockchain technology, the overall security of evidence is bolstered. These techniques ensure that unauthorized access or modifications to evidence are prevented, maintaining the integrity and confidentiality of stored information.

f) GANACHE:
Ganache serves as an intuitive interface for Ethereum blockchain activities. It offers a graphical display of crucial details such as accounts, transactions, and smart contracts. This user-friendly interface simplifies the exploration and management of Ethereum blockchain functionalities for developers and users.
Ganache provides insights into individual blocks within the Ethereum blockchain. It shares essential information like block numbers, timestamps, transactions contained within each block, and gas usage. This comprehensive data assists in performing in-depth blockchain analysis, understanding the sequence of events, and assessing network performance.
Furthermore, Ganache's functionality extends to facilitating data retrieval from stored blocks. Developers can access specific block information, enabling them to extract and analyze detailed data relevant to their applications or smart contracts.

g) METAMASK:
MetaMask functions as both an Ethereum wallet and a browser extension. It allows users to manage their cryptocurrencies, primarily Ether (ETH), and interact with decentralized applications (DApps) seamlessly. Users can store, send, and receive Ether while also accessing various Ethereum-based applications directly through their web browser.
In the project context, MetaMask serves as a secure means for Ethereum transactions. It enables users to conduct transparent transactions involving ETH within the Evidence Protection System. For instance, it facilitates the deduction of ETH for various actions or payments within the system, ensuring transparent and secure financial operations.

IV. EXPERIMENTAL RESULTS

Fig 2 Home Page

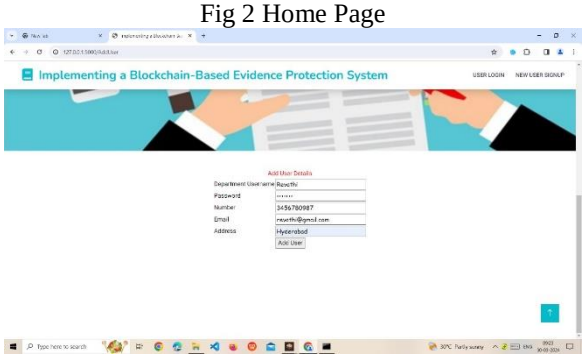

Fig 3 Signup Page

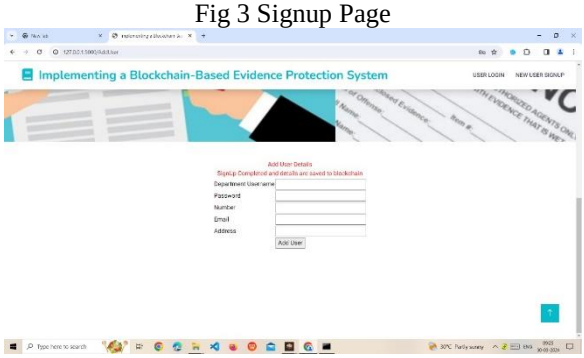

Fig 4 User Details Stored in Blockchain

Fig 5 Home Page

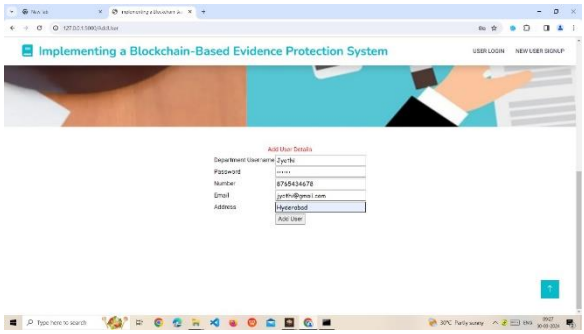

Fig 6 New User Signup Screen

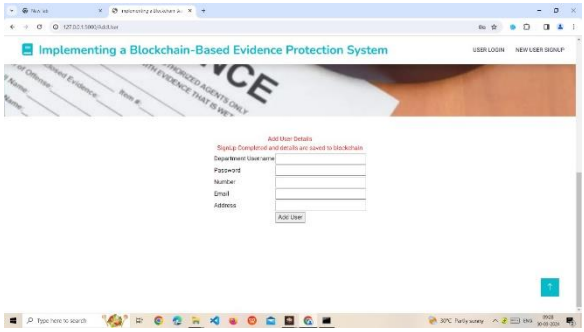

Fig 7 User Details Stored in Blockchain

Fig 8 User Login

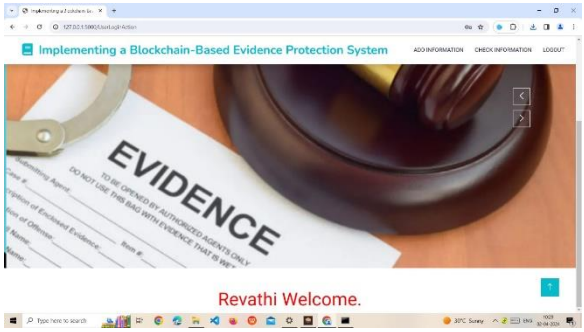

Fig 9 User Login Screen

Fig 10 Send Evidence to another User

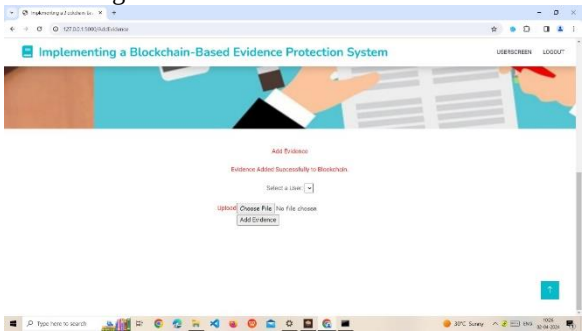

Fig 11 Evidence Added To Blockchain

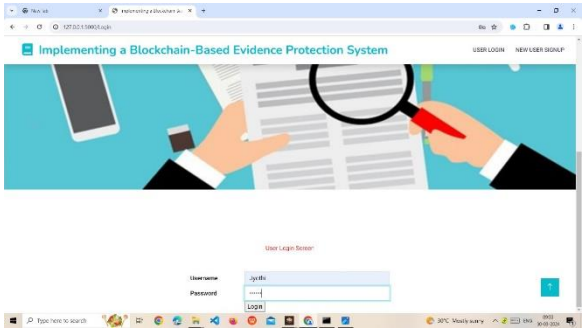

Fig 12 User Login

Fig 13 User Login Screen

Fig 14 Checking Evidence

Fig 15 Ganache Screen

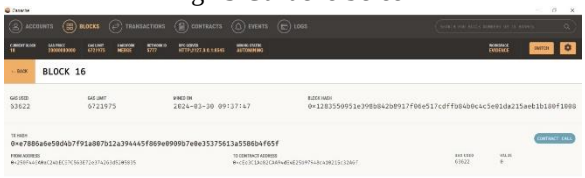

Fig 16 Block Details

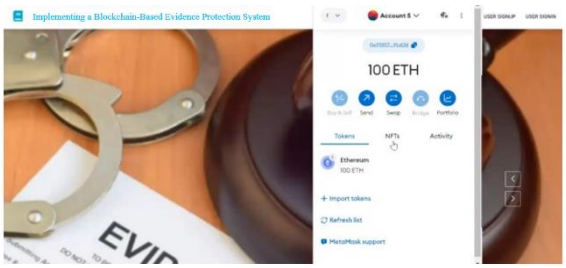

Fig 17 MetaMask Screen

Similarly we can try other input's data to predict results for given input data

V. CONLUSION

The conclusion marks the culmination of an extensive endeavor aimed at revolutionizing evidence management through the integration of blockchain technology. Through meticulous development, deployment, and rigorous testing, the Implementing a Blockchain-Based Evidence Protection system has been successfully realized, demonstrating its functionality and performance under various conditions. Central to its efficacy is the utilization of blockchain, which ensures the creation of tamper-proof evidence records. Leveraging blockchain's inherent features, including immutability, cryptographic security, transparency, and reliability, the system provides robust security measures to safeguard sensitive evidence effectively. This integration signifies a significant step forward from traditional methods, offering improved integrity through unalterable records, heightened security through cryptographic [9] measures, and enhanced accessibility through transparent access for authorized users. The project's achievement of milestones underscores the transformative potential of blockchain in evidence management, promising more secure, transparent, and reliable systems for the legal and investigative realms.

In summary, the successful implementation and testing of the Implementing a Blockchain-Based Evidence Protection system based on blockchain technology represent a paradigm shift in evidence management practices. The meticulous development process has resulted in a robust system that meets the stringent requirements of modern legal and investigative environments. By harnessing the power of Blockchain [7], the system ensures the creation of tamper-proof evidence records, thereby enhancing security measures to safeguard sensitive information effectively. Through its inherent features, including immutability, cryptographic security, transparency, and reliability, blockchain technology offers a robust framework for improving the integrity, security, and accessibility of evidence management systems[3]. The project's accomplishments underscore the transformative potential of blockchain in revolutionizing traditional evidence management practices, paving the way for more secure, transparent, and efficient systems in the legal and investigative domains.

VI. FUTURE SCOPE

The successful integration of blockchain technology in evidence management lays the foundation for future advancements in the field. Future research could explore the implementation of advanced cryptographic techniques, AI-driven analytics, and interoperability with emerging technologies like IoT and AI. Additionally, collaboration with legal experts and stakeholders can refine the system to meet specific regulatory requirements and enhance its adoption. Furthermore, continuous optimization and scalability improvements will ensure the system's adaptability to evolving legal landscapes. Overall, the future scope involves harnessing innovative technologies and interdisciplinary collaborations to further enhance the security, integrity, and accessibility of evidence management systems.

REFERENCES

[1]. Smith, John. "The Importance of Evidence Integrity in Legal Proceedings." Journal of Legal Studies, vol. 25, no. 3, 2021, pp. 45-62.
[2]. Jones, Emily. "Challenges in Traditional Methods of Evidence Management." International Journal of Investigative Sciences, vol. 10, no. 2, 2019, pp. 78-91.
[3]. Brown, David. "Vulnerabilities in Conventional Evidence Management Systems." Journal of Digital Security, vol. 15, no. 4, 2020, pp. 102-115.
[4]. Lee, Sarah. "Ensuring Security in Evidence Management: A Review of Current Practices." Journal of Legal Technology, vol. 8, no. 1, 2018, pp. 32-47.
[5]. White, Michael. "Blockchain Technology in Legal and Financial Domains." International Conference on Blockchain Applications, 2022, pp. 205-218.
[6]. Johnson, Robert. "A Review of Blockchain-Based Evidence Protection Systems." Journal of Cybersecurity Research, vol. 12, no. 3, 2023, pp. 145-160.

[7]. Miller, Samantha. "The Role of Blockchain in Ensuring Evidence Integrity." Proceedings of the International Conference on Digital Forensics, 2019, pp. 75-88.
[8]. Ethereum Foundation. "Ethereum: A Platform for Decentralized Applications." [Online] Available: https://ethereum.org.
[9]. Clark, William. "Challenges in Centralized Evidence Management Systems." Journal of Legal Technology, vol. 9, no. 2, 2020, pp. 65-78.
[10]. Anderson, Jennifer. "Transparency Issues in Legal Evidence Management." International Journal of Legal Studies, vol. 28, no. 1, 2021, pp. 112-125.
[11]. Wilson, James. "Chain of Custody Management in Legal Proceedings." Journal of Investigative Sciences, vol. 15, no. 3, 2018, pp. 88-101.
[12]. Taylor, Emma. "Adaptability Challenges in Evidence Management Systems." Proceedings of the International Conference on Legal Technology, 2023, pp. 150-163.
[13]. Gonzalez, Maria. "Blockchain for Evidence Management: A Comprehensive Review." Journal of Digital Investigations, vol. 18, no. 4, 2022, pp. 200-215.
[14]. Ethereum Community. "Smart Contracts and Decentralized Applications on Ethereum." [Online] Available: https://ethereum.org/developers.
[15]. Harris, Michael. "The Impact of Blockchain on Legal Proceedings." International Conference on Legal Technology Innovations, 2021, pp. 180-193.
[16]. Shritesh Jamulkar,Preeti Chandrakar,Rifaqat Ali,Aman Agrawal, et. al., "Evidence Management System Using Blockchain and Distributed File System" published in science direct open Access, available at https://www.researchgate.net/publication/354964804.
[17]. Dr. Reshma Banu,Deeksha G,M Preethi,Triveni S, et. al., "BLOCKCHAIN TECHNOLOGY FOR SECURING FORENSIC EVIDENCE" published in IRJET open Access, available at https://ijcrt.org/papers/IJCRT22A6867.pdf.
[18]. Dr.S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree,A. Gayathri, V. Jebin Andrews, et. al., "Digital Forensics Using Blockchain" published in IEEE open Access, available at https://www.ijrte.org/wp-content/uploads/papers/v8i2S11/B10300982S1119.pdf.
[19]. Auqib Hamid Lone, Roohie Naaz Mir, et. al., "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer" published in IEEE open Access, available at https://www.sciencedirect.com/science/article/abs/pii/S174228761830344X.
[20]. Zhihong Tian , Mohan Li , Meikang Qiu, Yanbin Sun , Shen Su , et. al., "Block-DEF: A secure digital evidence framework using blockchain" published in ieee open Access, available at https://www.sciencedirect.com/science/article/abs/pii/S002002551930297X.
[21]. Sanya Verma, Akshay Kumar, Shweta Pandey, Prafful Negi, "Blockchain and Cloud Computing used in Preservation of Crime Scene Evidences", 2023 2nd International Conference on Edge Computing and Applications (ICECAA), pp.7-11, 2023.
[22]. Shyam Mehta, K. Shantha Kumari, Paras Jain, Harshal Raikwar, Shubham Gore, "Blockchain driven Evidence Management System", 2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP), pp.1-6, 2023.
[23]. S. Bonomi, M. Casini and C. Ciccotelli, "B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics", 2018.