ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

Forensic Evidence Management Using Blockchain Technology

Dr. Mohammed Mustafa M[1]
Associate Professor
Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India

Kishore T C[2]
Student
Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India

Krithika N[3]
Student
Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India

Loga Bharathi M[4]
Student
Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India

Abstract:- In the realm of forensic investigations, the management of evidentiary artifacts is a critical aspect that influences the integrity and admissibility of evidence in legal proceedings. The trustworthiness of evidence can be jeopardized by traditional evidence management systems' frequent problems with data manipulation, unauthorized access, and lack of openness. Blockchain technology has surfaced as a viable approach to tackle these issues by offering a decentralized, transparent, and immutable foundation for data management in recent times. This paper explores the application of blockchain technology in forensic evidence management, highlighting its potential to enhance the security, integrity, and traceability of evidentiary artifacts throughout their lifecycle. By leveraging blockchain's inherent features such as cryptographic hashing, consensus mechanisms, and smart contracts, forensic practitioners can establish a tamper-proof chain of custody, ensure data integrity, and streamline the evidence management process. Moreover, blockchain-based evidence management systems offer benefits such as enhanced transparency, reduced reliance on centralized authorities, and improved collaboration among stakeholders. The paper discusses various use cases and implementations of blockchain technology in forensic evidence management, ranging from digital chain of custody records to decentralized forensic laboratories. Through a comprehensive analysis of the potential benefits and challenges, this paper aims to provide insights into the transformative impact of blockchain technology on forensic evidence management practices, paving the way for more secure, efficient, and trustworthy forensic investigations in the digital age.

Keywords:- *Blockchain, Forensic Evidence Management System, Cyber Threats.*

I. INTRODUCTION

The integration of blockchain technology into forensic evidence management represents a groundbreaking paradigm shift in the realm of data security. In an era characterized by rapid digitization and escalating cyber threats, traditional forensic evidence management systems are increasingly vulnerable to exploitation and compromise. However, the emergence of blockchain-based forensic evidence management systems offers a revolutionary solution to address these shortcomings. By harnessing the decentralized and immutable nature of blockchain technology, this innovative approach offers unparalleled levels of security, confidentiality, and accuracy in managing forensic evidence. The risk of tampering, manipulation, and data breaches is reduced by blockchain-based solutions, which disperse data throughout a network of nodes, in contrast to traditional centralized systems, which are vulnerable to single points of failure and illegal access. Through the use of cryptographic principles and decentralized consensus mechanisms, individuals gain unprecedented control over their digital identities, empowering them to safeguard their personalinformation from malicious actors and unauthorized intrusions. This decentralized approach not only enhances the security and integrity of forensic evidence but also ensures greater transparency and accountability in the management of digital identities. Moreover, blockchain technology's transparent and tamper- resistant features in still trust and confidence in the digital ecosystem, fostering a more resilient and user-centric approach to forensic evidence management. In essence, the integration of blockchain technology into forensic evidence management heralds a new era of digital data security. By leveraging the inherent strengths of blockchain technology, such as decentralization, immutability, and transparency, organizations and individuals alike can fortify their defences against cyber threats and safeguard the integrity of forensic evidence in an increasingly digitized world.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

- *Blockchain*

Block chain is a revolutionary technology that became well-known with the emergence of cryptocurrencies. It is a distributed and decentralized ledger system with broad applications in a number of sectors. Block chain is essentially a transparent and safe digital ledger that records and verifies transactions via a network of linked nodes.

Block chain is unique in that each connected block of data is cryptographically protected, preventing fraud and manipulation. This immutability makes the system unique. Because the technology is decentralized, there is no need for middlemen, which promotes participant confidence and lowers the possibility of data manipulation. Block chain is becoming more widely acknowledged for its potential to improve security, efficiency, and transparency in a variety of industries beyond finance, including as supply chain management and the healthcare industry. As a cornerstone of the decentralized digital future, block chain keeps redefining the ways in which data is exchanged, stored, and verified in the rapidly changing digital world.

- *Forensic Evidence Management System*

A The management of forensic evidence represents a critical aspect of modern investigative practices, encapsulating the meticulous handling, documentation, and preservation of evidentiary materials throughout the course of an investigation. At its core, a forensic evidence management system is tasked with safeguarding the integrity and authenticity of evidentiary items, ensuring that they remain unaltered and admissible in legal proceedings. In today's rapidly evolving digital landscape, the challenges associated with forensic evidence management are compounded by the proliferation of digital data and the increasing sophistication of cyber threats. As digital footprints and online profiles become integral components of data, the management of digital forensic evidence takes on added significance, requiring robust systems and protocols to address the unique complexities of digital evidence collection, analysis, and preservation. In an interconnected world where digital identities are subject to exploitation and manipulation, forensic evidence management systems must employ advanced technologies and methodologies to safeguard the integrity and confidentiality of evidentiary materials. By leveraging emerging technologies such as blockchain, forensic evidence management systems can enhance the security, transparency, and accountability of the evidentiary process. Blockchain's decentralized and immutable ledger provides a tamper-proof record of forensic evidence, ensuring its integrity and authenticity from collection to courtroom presentation. Additionally, blockchain technology enables secure and auditable chain of custody processes, enhancing accountability and traceability in the management of evidentiary materials.

- *Cyber Threats*

The prevalence of cyber risks has grown to be a significant problem in our technologically advanced and linked society, clouding the digital environment. Cyber threats are any number of malevolent actions carried out with the intention of jeopardizing the availability, confidentiality, or integrity of digital information by people, organizations, or even nation-states. These threats, which may range from complex hacking efforts to more typical phishing scams and malware assaults, take advantage of weaknesses in computer networks, human habits, and computer systems. Cybercriminals' tactics also evolve with technology , therefore it is critical for people, companies, and governments to continually improve their digital defences with vigilance and proactivity. The dynamic character of cyber threats highlights how crucial cybersecurity measures are to maintaining the privacy of sensitive and personal data, the dependability of vital infrastructure, and public confidence in our networked digital environment.

II. LITERATURE REVIEW

- *Hyperledger Frameworks with a Special Focus on Hyperledger Fabric*

The article authored by Marija S. and colleagues delves into the expanding realm of the Blockchain market, highlighting its growing importance across various industries amidst evolving business dynamics. Initially, the authors provide a comprehensive introduction to Blockchain technology, elucidating its decentralized nature and cryptographic foundations. Shifting focus, the paper explores projects within the Linux Hyperledger Initiative, notably Hyperledger Fabric, a prominent framework within this ecosystem. Through meticulous analysis, the authors delve into Fabric's architecture, organizational implications, and key features like private channels and smart contracts, offering insights into secure transaction mechanisms. They also detail the flow of transactions within the Fabric network, enhancing understanding of its operational dynamics and transactional integrity. Bridging theory with practice, the paper presents a simulated business network scenario, demonstrating the development of a basic application for monetary exchanges using Hyperledger Fabric. This practical illustration underscores Fabric's utility in real-world scenarios. Overall, Marija S. and colleagues' work serves as a guide to Blockchain technology, providing valuable insights for researchers and practitioners navigating this complex landscape. By demystifying concepts and showcasing applications, the paper empowers stakeholders to harness Blockchain's transformative potential effectively. As Blockchain continues reshaping industries, this research contributes to understanding its role in driving decentralized innovation.

- *A Decentralized Digital Identity Architecture*

Geoff Goodell and co-authors present a profound critique of centralized digital identity management, advocating for a decentralized, user-centric approach in their seminal paper. They highlight the failure of traditional systems to safeguard privacy and autonomy in the digital age, emphasizing the importance of human rights principles. Central to their argument is the concept of self-sovereign identity, where individuals have full control over their digital identities. They propose foundational principles for digital identity systems, including privacy by design and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

user-centricity. The authors explore emerging technologies like blockchain and decentralized identifiers, offering solutions for identity verification and data sharing. Additionally, they discuss the societal implications of decentralized identity systems, such as addressing identity theft and digital exclusion. Real-world applications, from identity wallets to voting systems, demonstrate the versatility of decentralized solutions. In conclusion, Goodell and colleagues envision a future where decentralized identity empowers individuals, protects their rights, and fosters inclusivity. Their paper calls on policymakers and technologists to embrace decentralized identity as a means to create a more equitable digital society.

- *Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging*

In this research, Yixuan Zhu et al. have proposed Blockchain is an ever-expanding collection of records, or blocks, connected and safeguarded by encryption. A timestamp, transaction data, and a hash pointer serving as a link to a previous block are normally included in every block. Blockchains are by their very nature resistant to data alteration. The blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." A blockchain is usually maintained via a peer-to-peer network that follows a common protocol for verifying new blocks in order to function as a distributed ledger. Once recorded, the data in a block cannot be changed backward without changing all blocks that come after it, which calls for the majority of the network to operate together. Digital money, like Bitcoin, is the most straightforward and widely used blockchain application. Bitcoins, in contrast to conventional money, are totally virtual. Coins, either real or digital, do not exist in and of themselves. In transactions when value is transferred from sender to receiver, the coins are inferred. Bitcoin users own keys that enable them to authenticate transactions inside the network, releasing the value so they may spend it or give it to another person. Usually, each user's computer has a digital wallet where such keys are kept. The sole need to spend bitcoins is to have the key that unlocks the transaction, giving each user complete power. These days, an increasing number of businesses and entrepreneurs are utilizing blockchain in finance records, medical records, and other records management activities, like identity management, transaction processing, documenting provenance, or food traceability, due to its decentralization, trustlessness, collective maintenance, and dependability.

- *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*

In their seminal paper, Elli Androulaki and colleagues delve into Fabric, an innovative modular and extensible open-source system designed for deploying and managing permissioned blockchains. Positioned as a flagship project under the Hyperledger umbrella hosted by the Linux Foundation, Fabric represents a significant leap forward in distributed ledger technology. Its modular architecture, a departure from traditional monolithic blockchain systems, enables developers to seamlessly integrate custom consensus protocols and components tailored to specific use cases. This flexibility empowers organizations to design bespoke blockchain solutions optimized for their unique business needs, fostering innovation and digital transformation. Fabric's support for modular consensus protocols further enhances its appeal, allowing organizations to tailor the blockchain network's consensus mechanism to align with their trust models and operational requirements. Moreover, Fabric's compatibility with standard programming languages eliminates the need for platform-specific smart contract languages, thereby lowering the barrier to entry for developers and accelerating blockchain adoption. Beyond its technical prowess, Fabric embodies an ethos of openness, collaboration, and community-driven innovation within the Hyperledger ecosystem. Through continuous evolution and adaptation, Fabric remains at the forefront of distributed ledger technology, poised to redefine enterprise blockchain and empower organizations to thrive in the digital age. Androulaki et al.'s paper serves as a seminal contribution to the field, illuminating the path towards a more inclusive, interoperable, and scalable blockchain ecosystem, where innovation knows no bounds.

- *B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics*

In their groundbreaking paper, Silvia Bonomi and colleagues delve into the intricate realm of digital forensics, emphasizing the paramount importance of effective evidence management—a cornerstone of successful investigations and legal proceedings. Central to digital forensics is the meticulous management of evidentiary artifacts, encompassing activities from collection to presentation in court, known as the Chain of Custody (CoC). This process ensures the integrity and admissibility of evidence despite passing through multiple stakeholders. The CoC process requires stringent protocols at each stage to prevent tampering, contamination, or unauthorized access. Evidentiary integrity, upheld through rigorous documentation and tracking mechanisms, underpins the reliability of digital evidence in legal proceedings. Multi-stakeholder involvement necessitates effective collaboration and communication to safeguard the evidential chain. In the digital age, managing evidence is further complicated by the dynamic nature of digital data. Bonomi et al. propose a comprehensive framework for digital evidence management, integrating advancements like blockchain and cryptographic hashing to enhance security and integrity. Interdisciplinary collaboration and knowledge sharing are advocated to promote consistency and reliability in evidentiary practices. Overall, the paper provides invaluable insights into navigating evidence management complexities, ensuring the integrity and admissibility of digital evidence in legal proceedings, and advancing the field of digital forensics.

III. EXISTING SYSTEM

Recognizes the critical role of evidence in forensic science, emphasizing its significance in solving cases and delivering justice by preventing alterations. Highlights the essentiality of the Chain of Custody process, underscoring that its failure may render evidence inadmissible in court, leading to potential case dismissal. Advocates for a digital

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

forensic evidence management system, citing environmental friendliness as a compelling reason for transitioning from traditional methods. Proposes the use of Hyperledger Fabric, a consortium blockchain framework, to digitally distribute and chronologically record forensic transactions, ensuring security and transparency. Aims to develop a framework based on Hyperledger Fabric concepts and proposes an algorithm to implement blockchain technology, specifically tailored for digitalizing forensic evidence management and maintaining the Chain of Custody.

IV. PROPOSED SYSTEM

The solution under consideration is a complete Forensic evidence management system that utilizes block chain technology and the SHA-256 algorithm to improve data integrity. It includes an easy-to-use Login module for safe authentication, a User Signup module for establishing accounts with necessary personal information, and a Home module that shows important block chain data. The Keys module generates public and private keys, which are necessary for safe transactions and provide strong cryptographic security. By creating a digital identity for users, the Data module improves verifiability and privacy. Finally, private keys for financial transactions are securely managed by the Authenticate module. Through the integration of various components, the system offers a transparent and decentralized structure that protects individual identities and guarantees data integrity within an unchangeable blockchain framework. By reducing the dangers connected with centralized forensic evidence management, this strategy provides users with a dependable and safe option in the constantly changing digital environment.

- *Login*

By requiring a username and password, the login module offers banks and users a safe authentication method. In order to customize access rights, it differentiates between normal users and banks based on responsibilities.

- *User Sign-Up*

Through the collection of necessary data, including first and last name, email address, cell phone number, username, and password, user registration makes it easier to create new accounts. The basis for user involvement in the block chain-based security system is laid forth in this module**.**

- *Home*

The Home module, which shows important details for every block, contains all of the block chain system's essential features. This contains the hash of the previous block, the hash of the current block, the block number, the timestamp, the contents, and the nonce (a cryptographic integer). By gaining access to the block chain's structure, users may verify the accuracy of the data contained within.

- *Keys*

In order to ensure cryptographic security, public and private keys must be generated via the Keys module. These keys are essential for maintaining the secrecy and authenticity of system communications and transactions.

- *Data*

The purpose of the Data module is to provide users in the block Chain system a digital data. In order to protect user privacy, facilitate safe transactions, and create a distinct and authenticated presence on the block chain, this digital identity is essential.

- *Authenticate*

A user's private key is stored and managed in the Authenticate module. This is an essential component of safeguarding their Authenticate access on the block chain. By guaranteeing the integrity and secrecy of financial transactions, this module strengthens the user's digital data's overall security.

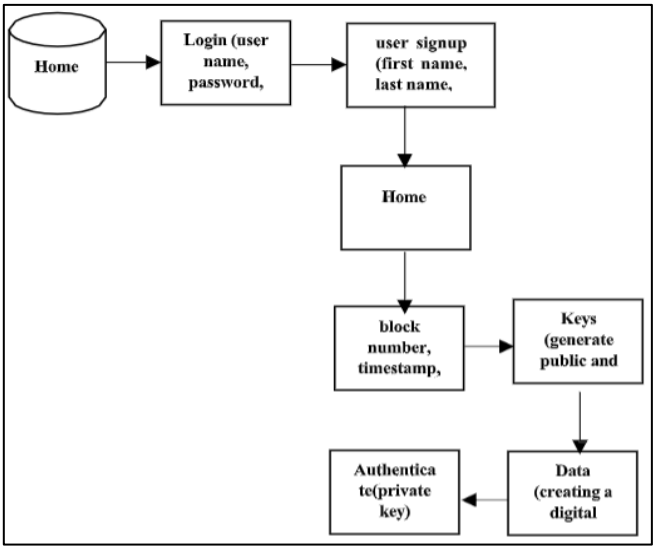

Fig 1 System Architecture Algorithm Details

A text or data file may be signed using the SHA 256 technique, often known as a digest. A text may be signed with a nearly unique 256-bit (32-byte) signature using SHA-256. A hash is a cryptographic "one-way" characteristic that has a set size for all source text sizes; unlike encryption, it cannot be decoded back to the original text. Because of this, it's perfect for comparing "hashed" copies of texts instead of decrypting them to get the original version.

- *Basic Initialization will be done for 8 Items*

- Step 1: Information is a array 8 things in length where everything is 32 bits.
- Step 2: out is array 8 things in length where everything is 32 bit.
- Step: 3 Compute all the capacity boxes and store those qualities. Allude to them by work name

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

- Step: 4 Store input, right moved by 32 bits, into out. Now, in the out exhibit, E is an inappropriate worth and A is unfilled
- Step: 5 Store the capacity boxes. Presently we have to compute out E and out A. note: Supplant the modulo orders with a bitwise AND 2^ (32-1)
- Step: 6 Store (Input I + CH + ((XT+YT) AND 2^31)) AND 2^31 As Mod1
- Step: 7 Store (Sum1 + Mod1) AND 2^31 as Mod2
- Step:8 Store (b + Mod2) AND 2^31 into out E Presently out E is right and all we need is out A
- Step: 9 Store (NA + Mod2) AND 2^31 as Mod3
- Step:10 Store (Sum0 + Mod3) AND 2^31 into output.

V. RESULT ANALYSIS

The suggested approach shows a significant increase, obtaining an accuracy rate of 88%, compared to the present algorithm's 75% accuracy rate. This improvement points to a significant improvement in the suggested algorithm's ability to handle and analyze data effectively or carry out its intended function. Numerous variables, including optimization approaches, algorithmic modification, or the incorporation of more reliable data preparation methods, may contribute to the suggested algorithm's increased accuracy. This improvement in accuracy highlights the suggested algorithm's ability to provide more dependable outcomes and favourably impact its targeted application area.

Table 1 Comparison Table

Algorithm	Accuracy
Existing	75
Proposed	88

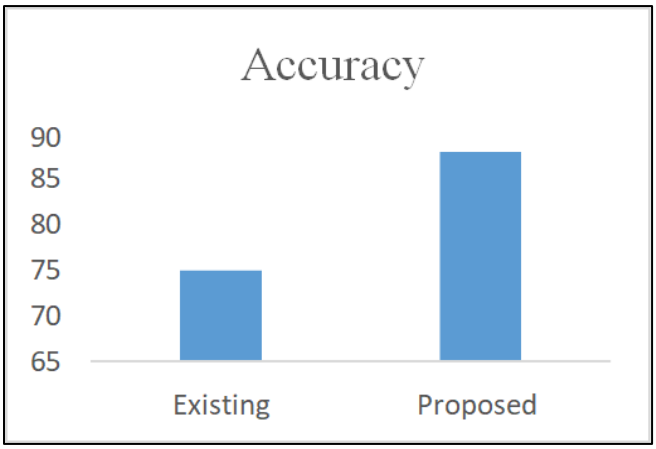

Fig 2 Comparison Graph

VI. CONCLUSION

To sum up, the suggested blockchain-based SHA-256 encryption Forensic evidence management system offers a strong and creative response to the problems associated with protecting digital identities. The system assures data integrity, user privacy, and secure financial transactions in addition to establishing a decentralized and transparent framework via the integration of modules including Login, User Signup, Home, Keys, Data , and Authenticate. User-friendly input and output interfaces are given priority in the design, which improves usability and accessibility. The system's objective is to mitigate the dangers associated with centralized forensic evidence management and promote confidence in an increasingly digital environment by offering a dependable and robust platform for users and banks, via methodical testing and deployment. Because of the thorough methodology used throughout the development and implementation phases, the system is positioned as a viable and efficient means of handling the ever-evolving complexity of Forensic evidence management.

FUTURE WORK

The personal identification security system based on blockchain may be improved in the future by being innovative and adjusting to new technology. Integrating smart contracts and sophisticated consensus techniques might improve the security and usefulness of the system even further. Examining the integration of verified credentials and decentralized identifiers (DIDs) might improve the interoperability and scalability of digital identities. In addition, the system may benefit from investigating biometric authentication techniques to offer one more degree of user verification.

REFERENCES

[1]. R. Kumar, A. Malik, and V. Ranga, "Identification Verification System via Blockchain Technology," Nov. 2022, vol. 256, art. no. 109762, Knowledge-Based Systems.

[2]. BPDIMS: A Blockchain-based Personal Data and Identity Management System, W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang, Compute. Secure., vol.112, Jan.2022, Art. no.102537.

[3]. "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," by J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bubley, and J. Kusuma June 2021, Telecom Policy, vol. 45, no. 5, Art. no. 102127 In February 2021, B. A. Tama and S. Lim published "Blockchain-based Identity Management with Mobile Device" in Computer Science and Engineering Review, vol. 39, art. no. 100357.

[4]. "Blockchain-Based Identity Management Systems: A Review," by S. Lei, C. Xia, Z. Li, X. Li, and T. Wang IEEE Trans. Netw. Sci. Eng., Oct. 20, 2021, vol. 8, no. 4, pp. 3257–3274

[5]. "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," by Y. Cheng, Y. Xu, H. Zhong, and Y. Liu IEEE Internet Things Journal, Jan. 2021, vol. 8, no. 1, pp. 144–155.

[6]. "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network," by X. Li, M. Zhu, L. T. Yang, M. Xu, Z. Ma, C. Zhong, H. Li, and Y. Xiang IEEE Transactions on Dependable Secure Computing, vol. 18, no. 4, July/Aug. 2021, pp. 1591–1604

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR354

[7]. A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain, Y. Zhou, G. Cheng, S. Jiang, and M. Dai, Compute. Netw., vol. 174, Jun. 2020, Art.no.107247.
[8]. "Blockchain for Identity Management," G. Kumar, K. Thakur, and M. R. Ayyagari, J. Super compute., vol. 76, no. 11, pp. 8938–8971, Nov. 2020
[9]. "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," by B. A. Tama, L. Nkenyereye, S. M. R. Islam, and K. Kwak IEEE Access, volume 8, 2020, pages 24120–24134.