International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 03 | Mar 2024 www.irjet.net p-ISSN: 2395-0072

Preserving-Integrity-of-Forensic-Evidence-using-Blockchain-Technology

Mrs.Diana.S.Steffi, S.Ramu, G.Harish, R.Saranraj, S.Gughan

[1]*Assistant Professor, Department of Computer Science and Engineering, Christ College of Engineering and Technology*
[2,3,4,5,6] *Department of Computer Science and Engineering, Christ College of engineering and Technology*

ABSTRACT

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 of 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:

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. This includes the proper seizure of devices, secure exhibit handling, meticulous data collection, and preservation protocols, as well as thorough examination and investigation techniques. By adhering to these principles, forensic investigators not only ensure the reliability of the evidence but also facilitate the establishment of a clear and unbroken chain of custody, which is essential in legal proceedings. Ultimately, their expertise in these areas contributes significantly to the successful resolution of cyber-attacks and digital crimes, while upholding the principles of justice and adherence to legal standards. After the seizure and preservation of evidence, the next crucial step in a digital forensic intelligence investigation is the examination phase. This phase involves the use of specialized forensic software and hardware to create a complete copy of all digital data from the collected devices, a process known as imaging. The imaging serves the dual purpose of preserving the original device as an evidence exhibit while leaving the imaged version available for forensic testing and analysis. This separation is essential to ensure that the original evidence remains untouched and uncontaminated throughout the investigation. Working in collaboration with our clients, the analysis phase of the digital forensic intelligence investigation begins with the thorough interrogation of the collected data. During this stage, forensic experts meticulously examine the imaged data to uncover critical information and insights. This may involve the recovery of deleted files, the identification of malicious software or cyberattack vectors, and the reconstruction of digital activities and timelines. The analysis phase is a pivotal step in the investigative process, as it aims to answer critical

questions, identify culprits, and provide the necessary evidence to support legal proceedings. It requires a combination of technical expertise, attention to detail, and a deep understanding of digital forensic methodologies to extract actionable intelligence from the data.

BLOCKCHAIN

A blockchain is a revolutionary technology that serves as a distributed database, designed to maintain a continuously growing and immutable list of ordered records, often referred to as "blocks." What sets it apart is its use of cryptography to secure and interconnect these blocks. Each block within the chain contains several crucial elements, including a cryptographic hash of the preceding block, a timestamp marking when the block was added to the chain, and transaction data specific to that block. This fundamental structure ensures that the information stored in a blockchain is secure, transparent, and tamper-proof. One of the defining characteristics of a blockchain is its decentralized and distributed nature. Unlike traditional centralized databases, a blockchain operates across a network of many computers, often referred to as nodes. This decentralization ensures that no single entity has complete control over the blockchain, making it resistant to manipulation and fraud. Moreover, the public nature of a blockchain means that anyone can participate in its network, view its contents, and contribute to its maintenance. The immutability of a blockchain is another key feature. Once a block is added to the chain, it becomes incredibly difficult to alter the information within it. This is due to the cryptographic links between blocks and the consensus mechanism used by the network. Any retroactive changes require the alteration of all subsequent blocks, which is computationally infeasible and would require the consensus of the majority of network participants. As a result, the data stored in a blockchain is considered highly secure and trustworthy, making it a valuable tool for a wide range of applications beyond just cryptocurrency, such as supply chain management, voting systems, and digital identity verification.

II. Literature survey:

Privacy Preservation for On-Chain Data in the Permissionless Blockchain using Symmetric Key Encryption and Smart Contract Riaz Ahmad Ziar, Syed Irfanullah, Wajid Ullah Khan, Abdus Salam [1] A privacy-preserving solution is proposed for permissionless blockchains, focusing on user control of transaction data while addressing on-chain data privacy concerns. The system utilizes symmetric cryptography and Ethereum smart contracts. Data providers register authorized users in an access control list, and data consumers can verify their validity on this list. Upon successful validation, data consumers can request a security key from data providers to access confidential data. A smart contract between the data provider and consumer is executed, sending the key for access. These smart contracts are implemented in Solidity, and their performance is evaluated on the Ropsten test network.

MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture Abdullah Ayub Khan , Mueen Uddin , Aftab Ahmed Shaikh , Asif Ali Laghari , Adil E. Rajput [2] MF-Ledger creates a private network among stakeholders to facilitate secure and transparent digital forensic investigations. Before being recorded on the blockchain ledger, participating stakeholders exchange and agree upon various investigation activities. Digital contracts, also known as smart contracts, are employed and implemented through sequence diagrams to manage secure interactions among stakeholders during the investigation process. This architectural solution offers robust information integrity, prevention, and preservation mechanisms, ensuring the permanent and immutable storage of evidence (including the chain of custody) within a private, permissioned, and encrypted blockchain ledger. In essence, MF-Ledger enhances the security and trustworthiness of digital forensic investigations in the realm of multimedia, addressing the evolving challenges posed by the modern digital landscape.

Blockchain based Digital Forensics Investigation Framework Renuka B S [3] In response to the growing threat of tampering with digital forensic data, a comprehensive solution has been devised. This method combines several key technologies to ensure the integrity and provenance of valuable digital forensic data. First, the forensic data is hashed using the robust SHA-256 algorithm, providing a unique fingerprint for each piece of data. Next, the data is encrypted using the AES Rijndael algorithm, adding an extra layer of security. To store this highly secure and encrypted data, Blockchain technology is employed, ensuring immutability and tamper-resistance. The implementation of this solution is facilitated through a Windows application developed in Visual Studio, which serves as both the client and server components. On the server side, the AES Rijndael algorithm is utilized to encrypt the forensic data, and the encrypted data is stored in Blockchain blocks. Communication between the client and server applications is achieved through TCP remoting, ensuring efficient data exchange. For data management, ADO.Net is used to interface between the Windows application and a MySQL database. Overall, this integrated approach provides a robust defense against malicious activities aimed at compromising the integrity of digital forensic data.

Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications Gulshan Kumar, Rahul Saha[4] Digital forensic in Internet-of-Thing (IoT) paradigm is critical due to its heterogeneity

and lack of transparency of evidence processing. Moreover, cross-border legalization makes a hindrance in such process pertaining to the cloud forensic issues. This urges a forensic framework for IoT which provides distributed computing, decentralization, and transparency of forensic investigation of digital evidences in cross-border perspectives. To this end, we propose a framework for IoT forensics that addresses the above mentioned issues. The proposed solution called Internet-of-Forensics (IoF) considers a blockchain tailored IoT framework for digital forensics. It provides a transparent view of the investigation process that involves all the stakeholders (e.g., heterogeneous devices, and cloud service providers) in a single framework. It uses blockchain-based case chain to deal with the investigation process including chain-of-custody and evidence chain. Consensus is used for consortium to solve the problems of cross-border legalization. This is also beneficial for a transparent and ease of forensic reference. The programmable lattice-based cryptographic primitives produce reduced complexities. It shows benefits for power-aware devices and puts an add-on to the novelty of the presented idea. IoF is generic; hence, it can be used by autonomous security operation centers, cyber-forensic investigators and manually initiated evidences under chain-of-custody for man-made crimes. Security services are assured as required by the framework. IoF is experimented and compared with the other state-of-the-art frameworks. The outcomes and analysis prove the efficiency of IoF concerning complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysis.

A Cost-efficient IoT Forensics Framework with Blockchain Suat Mercan; Mumin Cebe; Ege Tekiner; Kemal Akkaya; Melissa Chang; Selcuk Uluagac [5] IoT devices have been adopted widely in the last decade which enabled collection of various data from different environments. Data storage poses challenges since the data may be compromised during the storage and the integrity might be violated without being noticed. In such cases, integrity and data provenance are required in order to be able to detect the source of any incident and prove it in legal cases. To address these issues, blockchain provides excellent opportunities since it can protect the integrity of the data thanks to its distributed structure. However, it comes with certain costs as storing huge amount of data in a public blockchain will come with significant transaction fees. In this paper, we propose a highly cost effective and reliable digital forensics framework by exploiting multiple inexpensive blockchain networks as a temporary storage before the data is committed to Ethereum. To reduce Ethereum costs, we utilize Merkle trees which hierarchically stores hashes of the collected event data from IoT devices. We evaluated the approach on popular blockchains such as EOS, Stellar, and Ethereum by presenting a cost and security analysis. The results indicate that we can achieve significant cost savings without compromising the integrity of the data.

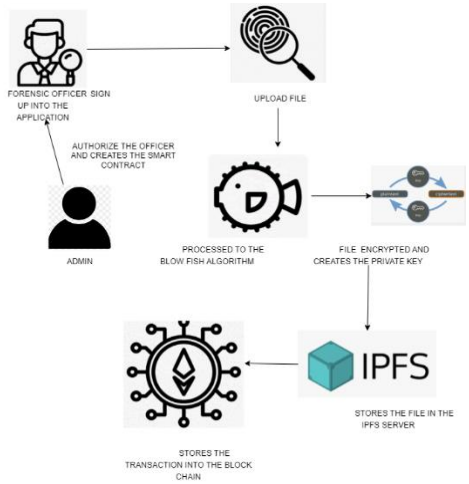
Probe-IoT: A public digital ledger based forensic investigation framework for IoT Mahmud Hossain; Ragib Hasan; Shams Zawoad [6] The increased deployment of Internet of Things (IoT) devices will make them targets for attacks. IoT devices can also be used as tools for committing crimes. In this regard, we propose Probe-IoT - a forensic investigation framework using a public digital ledger to find facts in criminal incidents in IoT-based systems. Probe-IoT collects interactions that take place among various IoT entities (clouds, users, and IoT devices) as evidence and stores them securely as transactions in public, distributed and decentralized blockchain network which is similar to the Bitcoin network. Probe-IoT presents a scheme that ensures integrity, confidentiality, anonymity, and non-repudiation of the evidence stored in the public ledger. Furthermore, during the investigation of a malicious incident, Probe-IoT provides a mechanism to acquire evidence from the ledger and verify the authenticity and integrity of the obtained evidence.

III. PROPOSED METHODOLOGY:

In the realm of cybercrime investigations, digital evidence serves as the linchpin for connecting suspects to alleged criminal activities. While the use of blockchain technology to store digital evidence offers tamper-resistance and immutability, a notable limitation has been the absence of encryption for the stored data, leaving it vulnerable to unauthorized access and compromise. The proposed solution seeks to address this security gap by incorporating the Solidity programming language for smart contracts and implementing the BLOWFISH (BF) encryption algorithm. The BF encryption algorithm plays a crucial role by encrypting the digital evidence files before they are stored in the blockchain. This encryption process transforms the data into an unreadable format, rendering it indecipherable without the appropriate decryption key. The act of encrypting data prior to storage in the blockchain introduces an additional layer of security. Even in the event that an attacker gains access to the blockchain, they would be unable to decipher the encrypted data without the encryption key. This measure significantly reduces the risk of data tampering, unauthorized access, and compromises of digital evidence, thereby enhancing the overall security of digital evidence in the context of cybercrime investigations. It ensures that the integrity and confidentiality of this critical information are upheld throughout the investigative process, providing a more robust and secure foundation for building legal cases and pursuing justice. **ADVANTAGE OF THE PROPOSED SYSTEM**

The encryption of digital evidence before its storage in the blockchain establishes a critical layer of security. It ensures that the data remains in an unreadable format without access to the decryption key, effectively preserving the evidence's integrity and confidentiality.

In the event of an unauthorized user gaining access to the blockchain, they would be thwarted by the encryption. Without the appropriate decryption key, the encrypted data remains inaccessible, mitigating the risk of data breaches and unauthorized access to sensitive evidence. The combination of the blockchain's inherent tamper-resistance, reinforced by encryption, forms a formidable defense against data tampering. Malicious actors are confronted with significant barriers to altering or manipulating the encrypted evidence, making it an extremely challenging task. This integrated approach not only enhances the security and trustworthiness of digital evidence but also bolsters the overall reliability of the blockchain as a secure repository for sensitive information, crucial in the context of cybercrime investigations and legal proceedings.



Architecture is designed to fortify the security of digital evidence in cybercrime investigations by integrating blockchain technology, Solidity programming language for smart contracts, and the BLOWFISH (BF) encryption algorithm. At the core of the architecture is a decentralized blockchain network where digital evidence is stored in an immutable and tamper-resistant manner. Smart contracts, programmed in Solidity, govern the encryption and storage process. When digital evidence files are submitted, they undergo encryption using the BLOWFISH algorithm before being securely stored on the blockchain. The encrypted data, now indecipherable without the proper decryption key, adds a crucial layer of protection against unauthorized access. Users with the appropriate authorization can interact with the smart contracts to submit, retrieve, and manage digital evidence. The decentralized nature of the blockchain ensures that no single point of failure exists, enhancing the overall resilience of the system. This architecture not only safeguards digital evidence against tampering and compromise but also facilitates a transparent and auditable process in cybercrime investigations, thereby establishing a robust and secure foundation for the legal proceedings.

IV. RESULT AND DISCUSSION:

Data Encryption Module (Blow Fish Encryption)

The Data Encryption Module plays a pivotal role in safeguarding sensitive data. Its primary responsibility is to apply encryption to the information before it is stored within the blockchain. In this context, Blowfish encryption, a well-regarded symmetric-key block cipher, takes center stage. It serves as the cryptographic method of choice for ensuring the confidentiality and security of the data. Blowfish encryption is designed to transform the data into an unreadable and seemingly random format, a process known as ciphertext. The transformation is carried out in such a way that only those with the appropriate decryption key can reverse this process and make the data readable again. This ensures that even if unauthorized parties gain access to the stored data, they will be confronted with a seemingly incomprehensible jumble of characters, rendering the information secure from prying eyes. The encryption key, held by authorized users or systems, is the only means to unlock and decipher the data, reinforcing the data's confidentiality and security within the blockchain. Blockchain Storage Module: This module manages the secure storage of encrypted data on the blockchain. It utilizes the blockchain's decentralized and immutable nature to prevent unauthorized access or tampering. Data stored in the blockchain is cryptographically protected and can be traced back to its source, ensuring data integrity and trustworthiness.

Access Control Module

The Access Control Module is the linchpin of system security. It plays a pivotal role in defining and enforcing user interactions within the system, with a keen focus on user permissions. Its primary function is to ensure that only individuals with authorized access are allowed to interact with the system and its stored data. Access control sets the boundaries for what each user can and cannot do, such as accessing, modifying, or retrieving data, making it a critical security layer. By regulating these user permissions, the Access Control Module acts as a gatekeeper, preventing unauthorized access to sensitive information. It works to minimize the risk of data breaches, data manipulation, or any malicious activity that could compromise the confidentiality and integrity of stored data. This security layer is essential in safeguarding sensitive information and maintaining the trustworthiness of digital evidence, making it an indispensable component in systems dedicated to digital forensics and data security.

Authentication and Authorization Module

Authentication: This process is about verifying the identity of a user. It ensures that the person trying to access the system is indeed who they claim to be. This is typically achieved through the use of credentials like usernames and passwords, biometric data (such as fingerprints or facial recognition), or multi-factor authentication (combining multiple methods for added security). The goal of authentication is to prevent unauthorized individuals from gaining access to the system.

Authorization: Once a user's identity is confirmed through authentication, authorization comes into play. Authorization determines what actions or resources that authenticated user is allowed to access within the system. It defines the permissions and privileges associated with each user's role or profile. For example, some users may have read-only access, while others may have read and write permissions. Authorization ensures that users can only perform actions that they are explicitly allowed to undertake.

Together, these two modules work in harmony to control user access effectively. Authentication establishes who you are, while authorization specifies what you are allowed to do. This dual-layered approach helps maintain the security and integrity of a system by ensuring that only authorized users can perform specific actions or access certain data, contributing to a robust and controlled user access environment.

Reporting and Logging Module

The Reporting and Logging Module is an indispensable component of any digital system, particularly in contexts where security, accountability, and traceability are paramount. This module serves as the meticulous recorder of all activities occurring within the system. It diligently captures and stores a comprehensive log of user interactions, data access, system changes, and other relevant events. These logs are not merely data entries; they are the system's memory, holding a record of who accessed the data, what actions they executed, and precisely when these actions occurred. The significance of this module cannot be overstated, as it plays a multifaceted role in ensuring the system's integrity and reliability. First and foremost, it bolsters accountability by providing a transparent and chronological account of user actions. This transparency is invaluable, particularly in forensic investigations and legal proceedings, as it helps establish a clear audit trail. In the event of security breaches, data tampering, or unauthorized access, these logs become an indispensable resource for identifying the culprits and understanding the extent of the breach. Moreover, the logs and reports generated by this module are instrumental for auditing and monitoring purposes. They empower administrators and security personnel to keep a vigilant eye on system activities, promptly detecting any irregularities or suspicious behavior. By doing so, they enhance the system's overall security and compliance with industry standards and regulations.

Integration with Digital Forensic Tools

This module facilitates the seamless integration of digital forensic tools and software. It allows investigators to retrieve, analyze, and cross-reference data from the blockchain with forensic evidence. This integration streamlines the investigative process and ensures that digital evidence is handled effectively within the system. These modules collectively create a comprehensive system for managing digital evidence, securing it with encryption, preserving its integrity through blockchain technology, controlling user access, maintaining detailed logs, and integrating with forensic tools for effective investigations.

PERFORMANCE ANALYSIS:

BLOW FISH ALGORITHM:

Your explanation provides a good overview of the distinction between symmetric and asymmetric key cryptography, as well as the classification of symmetric algorithms into block ciphers and stream ciphers. It correctly highlights that Blowfish is a symmetric key block cipher designed by Bruce Schneier in 1993. Blowfish's features, such as its 64-bit block size, variable key length (ranging from 32 to 448 bits), and the option to use variants with different numbers of rounds (up to 16 rounds), are well described. Additionally, mentioning its initial purpose to provide a patent and copyright-free encryption algorithm is insightful, as it has contributed to its widespread adoption.

Blowfish is a symmetric-key block cipher designed to be efficient in both hardware and software. It uses a variable key size and operates on fixed-size blocks of data. The parameters used in the Blowfish algorithm include the key size, the number of rounds, and the initial P-box and S-boxes.

KEY SIZE (K):

Blowfish supports variable key sizes from 32 to 448 bits. The key size is a multiple of 32 bits, ranging from 4 bytes (32 bits) to 56 bytes (448 bits).
The key is divided into subkeys, used in the encryption and decryption processes.

NUMBER OF ROUNDS (R):

Blowfish operates on data in a series of rounds. The more rounds used, the more secure the encryption, but it also increases computational complexity.
A recommended default is 16 rounds, but the algorithm can be configured with as few as 4 rounds or as many as 16 rounds.

INITIAL P-BOX AND S-BOXES:

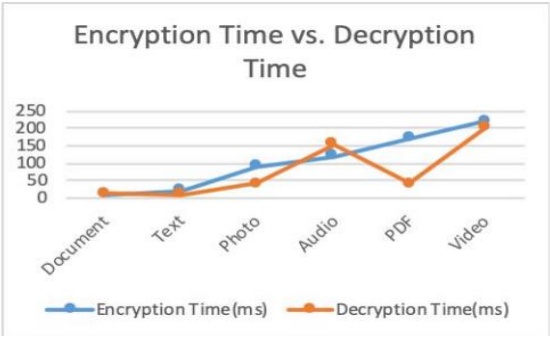
Blowfish uses a set of P-boxes (32-bit subkeys) and S-boxes (8x32-bit substitution boxes).

P-boxes: The P-boxes are initialized based on the digits of pi (π) and the fractional part of the square root of prime numbers. The initial P-box is denoted as P1, P2, ..., P18.

S-boxes: Blowfish uses four S-boxes each containing 256 32-bit entries. The initial S-boxes are initialized using the hexadecimal digits of pi (π). The initial S-boxes are denoted as S1, S2, S3, and S4.

Blowfish encryption and decryption use these parameters along with the subkeys derived from the key to perform a series of operations, including Feistel network operations, substitution-permutation network (SPN) structures, and XOR operations. The algorithm's flexibility and parameter choices make it adaptable for different security needs and hardware/software environments.

ENCRYPTION VS DECRYPTION TIME:



The observed difference in encryption and decryption times for various electronic data types, such as text, photo, and video files, suggests variations in the computational requirements of these processes. In general, symmetric key encryption algorithms, like Blowfish, often exhibit similar times for encryption and decryption due to their symmetric nature – the same key is used for both operations. However, the discrepancy in the case of PDF files, where decryption time is higher than encryption time, could be attributed to the specific characteristics of PDF file structures. PDF files often involve complex formatting, embedded images, and intricate layouts, which can result in larger file sizes compared to simple text or image files. During encryption, the algorithm might efficiently process and reorganize the data, leading to relatively lower encryption times. On the other hand, during decryption, the algorithm may encounter challenges in reconstructing the intricate PDF structure, resulting in increased decryption times. Additionally, the decryption process may involve more complex operations to restore the original format, contributing to the observed higher decryption times for PDF files. This discrepancy highlights the importance of considering the unique characteristics of each file type when evaluating the performance of encryption and decryption processes.

PROOF OF STAKE:

TX_{tr} is stored in IPFS and hash is stored in blockchain. The product hash (H_{pro}) includes the product type (P_{typ}), quantity (P_{quan}), price (P_{pri}), and place of origin (P_{ori}). When a product is confirmed to have been delivered from the seller to the buyer in a transaction, $Tx_{tr} = [ID_{pro}||H_{pro}||ID_{buy}||Sig_{buy}||PK_{buy}||Sig_{sell}||Pk_{sell}]$, where ID_{buy}, Sig_{buy}, and PK_{buy} represent the identifier, signature, and public key of the owner, respectively;

$$TXtr = \left[ID_{\text{pro}}||H_{\text{pro}}||ID_{\text{buy}}||\text{Sig}_{\text{buy}}||Pk_{\text{buy}}||\text{Sig}_{\text{sell}}||Pk_{\text{sell}}\right].$$

D_{buy}, Sig_{sell}, and PK_{sell} represent the identifier, signature, and public key of the seller, that is, the signature (Sig_{own}) and public key (PK_{own}) of the product owner in (1). The identity is required to be transformed in the process of product transaction, the owner of a transaction will be the seller in a subsequent transaction, and the buyer will become the owner of the product when the transaction is complete. After the consumer buys the product from the retailer, the seller creates the transaction order m_R

$$m_R = \Phi\left(m_t, \varsigma\left(SK_{\text{sell}}, m_t\right)\right).$$

Then, he/she verifies the user's signature based on the seller's public key. Secondly, the consumer creates the ring signature based on the assessment information and sends the to the blockchain. The blockchain verifies m_R and , and, upon successful verification, Info will be stored in IPFS, and H_{Info} will be stored in the blockchain network. In addition, the trust value

$$\text{Value}_{\text{trust}} = \frac{\sum\left(\alpha \cdot \text{score}_{\text{ser}} + \beta \cdot \text{score}_{\text{qual}}\right)}{\text{Total}_{\text{trans}}}, \quad \text{Total}_{\text{trans}} \geq n,$$

V. CONCLUSION:

In conclusion, 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. At its core, this system harnesses the power of blockchain and smart contracts to revolutionize key forensic processes, including evidence tracking, chain of custody management, and access control. By doing so, it not only enhances data security and integrity but also offers a remarkable boost in traceability, transparency, and operational efficiency. 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.

FUTURE WORK

Future work in this field holds the promise of further innovation and refinement. As technology and data continue to evolve, forensic investigations will need to adapt, incorporating advanced tools for handling complex digital evidence. The integration of artificial intelligence and machine learning can streamline the analysis of massive data sets, improving the efficiency of investigations. Additionally, research into more secure and efficient consensus mechanisms for blockchain integration, along with enhanced encryption techniques, can strengthen data protection. Furthermore, collaboration between forensic experts, legal professionals, and technology developers will be crucial to ensure that forensic systems keep pace with emerging challenges and maintain the highest standards of integrity and security. The ongoing commitment to staying at the forefront of technological advancements and the ever-changing landscape of digital evidence will be essential for the future of forensic investigations.

REFRENCES

- IoT Devices Installed Base Worldwide 2015–2025|Statista. Available online:https://www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/ (accessed on 29 December 2022).
- Xu, L.; Jurcut, A.D.; Ranaweera, P. Introduction to IoT Security; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]
- Li, S.; Qin, T.; Min, G. Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Trans. Comput. Soc. Syst. 2019, 6, 1433–1441. [CrossRef]
- Hanggoro, D.; Sari, R.F. A Review of Lightweight Blockchain Technology Implementation to the Internet of Things. Available online: https://ieeexplore.ieee.org/abstract/document/9042431/ (accessed on 29 December 2022).
- 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]
- 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]
- 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 (accessed on 29 December 2022).
- Panda, S.K.; Jena, A.K.; Swain, S.K.; Satapathy, S.C. Blockchain Technology: Applications and Challenges; Intelligent Systems Reference Library: Berlin, Germany, 2021. [CrossRef]
- Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The Revolution of Blockchain: State-of-the-Art and Research Challenges. Arch. Comput. Methods Eng. 2021, 28, 1497–1515. [CrossRef]
- Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. IEEE Internet Things J. 2020, 8, 1817–1829.
- Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Gener. Comput. Syst. 2021, 120, 13–25.
- NSL-KDD|Datasets|Research|Canadian Institute for Cybersecurity|UNB. Available online: https://www.unb.ca/cic/datasets/ nsl.html (accessed on 29 December 2022).
- Ramchoun, H.; Amine, M.; Idrissi, J.; Ghanou, Y.; Ettaouil, M. Multilayer Perceptron: Architecture Optimization and Training. Int. J. Interact. Multimed. Artif. Intell. 2016, 4, 26.
- Carstensen A, Bernhard J (2019) Design science research–a powerful tool for improving methods in engineering education research. Eur J Eng Educ 44(1–2):85–102 6. South African government, "Local government," [Online]. Available: https://www.gov.za/about-government/governmentsystem/local-government. Accessed 03 Nov 2022.
- Western cape government, "Municipalities in the Western Cape," [Online]. Available: https://www.westerncape.gov.za/ general-publication/municipalities-western-cape. Accessed 03 Nov 2022.