iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61074

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Securing Forensic Data Using Block Chain

Dr. M. Chandrakala[1], R. P. Saggithya[2], B. Sumithra[3], R. Indumaathi[4]
[1]*Head of The Department And Assistant Proffesor*
Idhaya College of Arts and Science for Women Pakkamudaiyanpet,Puducherry-605008.

Abstract: ***The incorporation of blockchain technology into forensic investigations represents a significant advancement, tackling critical challenges within the legal and criminal justice systems. Central to this integration are smart contracts, which automate and secure essential aspects of investigations. These self-executing agreements operate based on predefined rules, ensuring integrity and transparency in tasks such as evidence tracking, chain of custody management, and access control. A key advantage lies in the substantial enhancement of data security. Blockchain's cryptographic principles and decentralized structure make it highly resistant to unauthorized access and tampering, crucial in maintaining evidence integrity. Additionally, blockchain's immutability ensures the reliability of information; once recorded, data becomes virtually unalterable, providing an indisputable ledger of events. In summary, this innovative integration streamlines operations, reduces errors and disputes, and strengthens the trustworthiness of forensic investigations by offering an unforgeable and transparent chain of custody and evidence history within the legal and criminal justice framework.***
Keywords: forensic investigations, blockchain, data security.

I. INTRODUCTION

Forensic intelligence is crucial for investigating cyber-attacks and digital crimes, demanding specialized expertise in preserving and analyzing digital evidence. Forensic investigators follow strict methodologies and principles to uphold evidence integrity throughout the investigation. Maintaining evidence continuity ensures the trustworthiness and admissibility of evidence, establishing a transparent chain of custody for legal purposes. The examination phase involves duplicating digital data through imaging, safeguarding the original evidence for forensic examination. During analysis, experts meticulously scrutinize imaged data to unveil vital information like deleted files or cyberattack methods. This phase aims to provide actionable insights, identify perpetrators, and bolster legal proceedings. Successful analysis necessitates technical proficiency, meticulous attention to detail, and a profound grasp of digital forensic methodologies. Collaboration with clients is essential throughout the investigation to ensure thorough analysis and effective resolution of cyber incidents.

II. RELATED WORK

1) Privacy Preservation for On-Chain Data in the Permissionless Blockchain using Symmetric Key Encryption and Smart Contract [1] a existing solution aims to enhance privacy on permissionless blockchains by empowering users to control their transaction data, thereby mitigating on-chain privacy concerns. Employing symmetric cryptography and Ethereum smart contracts, the system operates by enabling data providers to register authorized users within an access control list. Subsequently, data consumers can verify their legitimacy against this list, ensuring secure access. Upon successful validation, consumers can request a security key from the data providers to unlock confidential data. This process is facilitated through the execution of smart contracts written in Solidity, enabling the secure exchange of keys. The performance of these smart contracts is assessed on the Ropsten test network to gauge their effectiveness in real-world scenarios.

2) MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture [2] MF-Ledger establishes a private network among stakeholders to facilitate secure and transparent digital forensic investigations. Prior to recording on the blockchain ledger, participating stakeholders engage in exchanges and agreements regarding various investigation activities. Through the utilization of digital contracts, also known as smart contracts, interactions among stakeholders during the investigation process are managed securely via sequence diagrams. This architectural solution ensures robust information integrity, prevention, and preservation mechanisms, guaranteeing the permanent and immutable storage of evidence, including the chain of custody, within a private, permissioned, and encrypted blockchain ledger. Essentially, MF-Ledger heightens the security and reliability of digital forensic investigations within the multimedia domain, adeptly tackling the evolving challenges presented by the modern digital landscape.

©IJRASET: All Rights are Reserved

3) Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems [3] This paper introduces a new framework called IoT forensic chain (IoTFC), which utilizes blockchain technology to enhance digital forensics (DF) investigations, particularly in the realms of Internet of Things (IoT) and social systems. By leveraging the decentralized nature of blockchain, IoTFC aims to improve the integrity and reliability of evidence collection, even when investigations span across different jurisdictions. It achieves this by providing proof of existence and preserving privacy during evidence examination, ensuring authenticity, immutability, traceability, resilience, and distributed trust among involved parties. IoTFC records crucial details of evidence identification, preservation, analysis, and presentation within blockchain blocks, ensuring traceability and provenance tracking. This transparency in the audit trail not only enhances trust in evidence items but also fosters confidence in the examiners conducting the investigations. Furthermore, the paper explores how blockchain can be employed for secure communication in defense applications, guaranteeing privacy through message signing with corresponding private keys. In essence, the decentralized nature of blockchain technology aligns well with the requirements of digital forensics, particularly in maintaining the integrity and traceability of evidence across diverse environments and applications, such as IoT and social systems.

4) Blockchain based Digital Forensics Investigation Framework [4] To counter the rising threat of tampering with digital forensic data, a comprehensive solution has been developed. This method amalgamates various technologies to safeguard the integrity and provenance of crucial digital forensic data. Initially, the forensic data undergoes hashing using the SHA-256 algorithm, generating a unique fingerprint for each piece of data. Subsequently, the data is encrypted using the AES Rijndael algorithm, enhancing its security further. Blockchain technology is then employed to store this highly secure and encrypted data, ensuring its immutability and resistance to tampering. The implementation of this solution is facilitated through a Windows application created in Visual Studio, functioning as both the client and server components. On the server side, the AES Rijndael algorithm is employed for encrypting the forensic data, which is then stored in Blockchain blocks.

5) A blockchain based digital forensics framework for IoT applications [5] A key feature of IoF is the use of a blockchain-based case chain to manage the investigation process, encompassing the chain-of-custody and evidence chain. Consensus mechanisms are employed to address cross-border legal challenges, ensuring transparency and facilitating forensic reference. Additionally, IoF utilizes programmable lattice-based cryptographic primitives to reduce complexities, particularly beneficial for power-efficient IoT devices, enhancing the novelty of the proposed framework. IoF's versatility enables its adoption by autonomous security operation centers, cyber-forensic investigators, and for managing manually initiated evidences under chain-of-custody protocols for various crimes. The framework guarantees security services as required, ensuring the integrity and confidentiality of digital evidence. Experimental evaluation and comparison with state-of-the-art frameworks demonstrate IoF's efficiency across multiple metrics including complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysis.

III. PROPOSED SYSTEM

Within cybercrime investigations, digital evidence is pivotal in linking suspects to alleged criminal activities. While blockchain technology ensures tamper-resistance and immutability for stored digital evidence, a notable drawback is the absence of encryption, leaving data vulnerable to unauthorized access and compromise.

To address this security gap, the proposed solution integrates the Solidity programming language for smart contracts and implements the BLOWFISH (BF) encryption algorithm. BF encryption plays a crucial role by encrypting digital evidence files before storage in the blockchain.

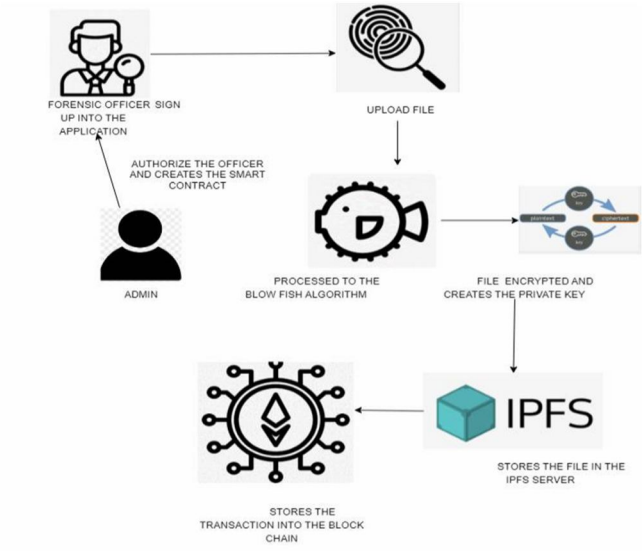
This process transforms data into an unreadable format, making it indecipherable without the appropriate decryption key. Encrypting data before storage introduces an additional layer of security. Even if attackers gain access to the blockchain, they cannot decipher the encrypted data without the encryption key.

This measure significantly mitigates risks of data tampering, unauthorized access, and compromises of digital evidence, enhancing overall security in cybercrime investigations.

It ensures integrity and confidentiality of critical information throughout the investigative process, establishing a more robust foundation for building legal cases and pursuing justice.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. ARCHITECTURE DIAGRAM



The architecture diagram presents a system designed to bolster the security and reliability of digital evidence in cybercrime investigations. It centers around a blockchain network, known for its decentralized nature and resistance to tampering, serving as the foundation for storing digital evidence securely. Smart contracts, developed using Solidity, are utilized to introduce various functionalities into the system. Before digital evidence is stored on the blockchain, it undergoes encryption using the BLOWFISH (BF) algorithm. This encryption step ensures that the data remains inaccessible and protected, even if unauthorized parties attempt to gain access to the blockchain. Furthermore, the architecture includes components responsible for managing access control and authentication. These mechanisms ensure that only authorized individuals have permission to access the blockchain network and the encrypted digital evidence, thereby enhancing overall security. Additionally, monitoring and logging functionalities are integrated to track and record access to the digital evidence. This allows for the detection of any suspicious activities and ensures transparency and accountability throughout the investigation process.

V. RESULT AND DISCUSSION

A. 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.

B. 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.

C. 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.

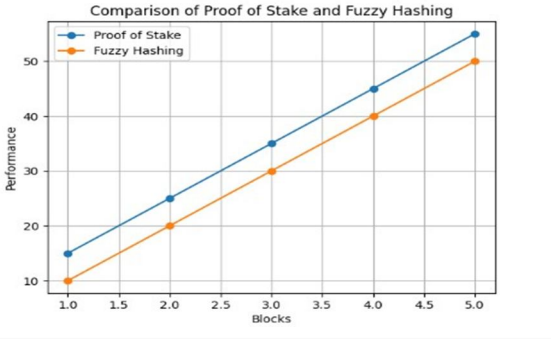
D. Reporting and Logging Module

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.

E. 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.

1) Comparison Of Fuzzy Hash And Proof Of Stack Algorithm

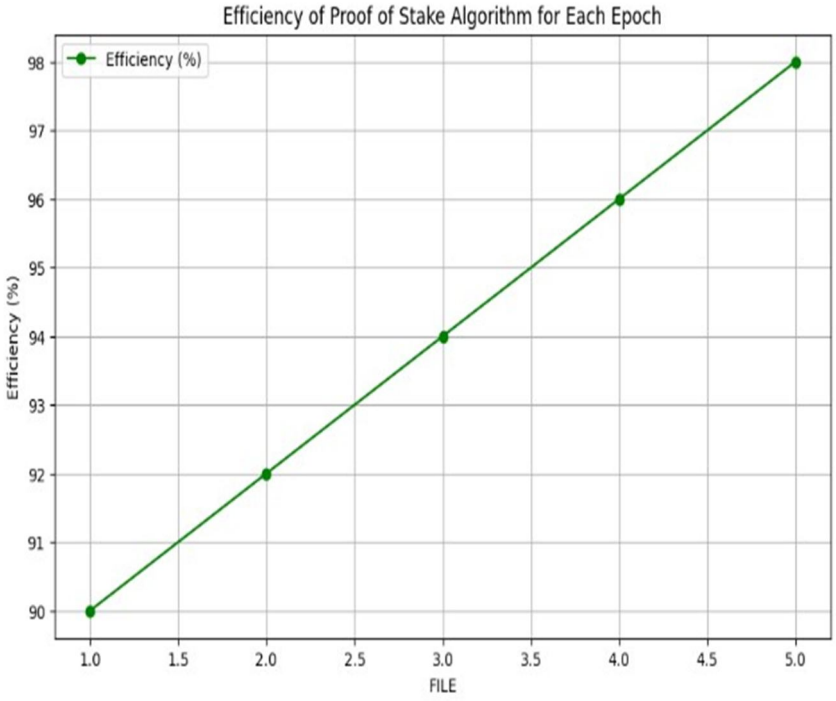


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

The comparison between Fuzzy Hashing and Proof of Stake (PoS) algorithms involves assessing their respective strengths and weaknesses in different contexts, particularly within the realms of cybersecurity and blockchain technology.

Fuzzy Hashing, a cryptographic technique, operates by generating unique hash values for data blocks, allowing for comparison between similar datasets while tolerating minor variations. It excels in identifying similar or identical files despite alterations, making it invaluable in malware detection, data deduplication, and digital forensics. Fuzzy Hashing's ability to detect similarities within datasets, even with slight modifications, enhances its utility in cybersecurity for identifying known threats and detecting file alterations. On the other hand, Proof of Stake is a consensus algorithm utilized in blockchain networks to validate transactions and secure the network. Unlike Proof of Work (PoW), which requires extensive computational resources, PoS selects validators based on the number of coins they hold and are willing to "stake" as collateral. PoS offers advantages such as reduced energy consumption, faster transaction processing, and increased scalability compared to PoW-based systems. However, PoS introduces potential centralization risks, as validators with more significant stakes have greater influence over network operations. When comparing Fuzzy Hashing and Proof of Stake, their applications and objectives differ significantly. Fuzzy Hashing primarily focuses on data integrity and similarity detection, crucial for cybersecurity and digital forensics. In contrast, Proof of Stake serves as a consensus mechanism within blockchain networks, aiming to ensure network security and transaction validation efficiently.

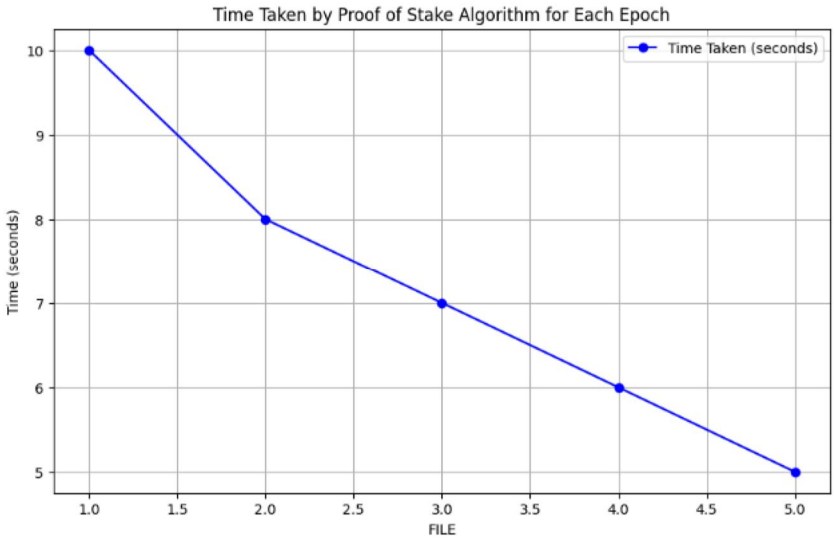
2) Efficency Graph For Proof Of Stack Algorithm



The efficiency graph for the Proof of Stake (PoS) algorithm illustrates the performance of the algorithm across different epochs. Each epoch represents a fixed period of time during which a set of validators is selected to validate transactions and create new blocks. The efficiency of the PoS algorithm, depicted as a percentage on the y-axis, measures how effectively the algorithm utilizes the resources available to achieve consensus and maintain network security. As shown in the graph, the efficiency of the PoS algorithm typically increases over successive epochs. This improvement can be attributed to several factors, including enhancements in the validator selection algorithm, optimization of network protocols, and increased participation and stake among validators. Higher efficiency indicates that the PoS algorithm is becoming more adept at selecting validators, validating transactions, and securing the network with minimal resource consumption. A rising efficiency curve signifies the algorithm's ability to achieve consensus more quickly and with fewer resources, leading to faster transaction processing times and improved overall network performance. Conversely, a declining or stagnant efficiency curve may indicate inefficiencies in the PoS algorithm, such as suboptimal validator selection or increased network congestion.

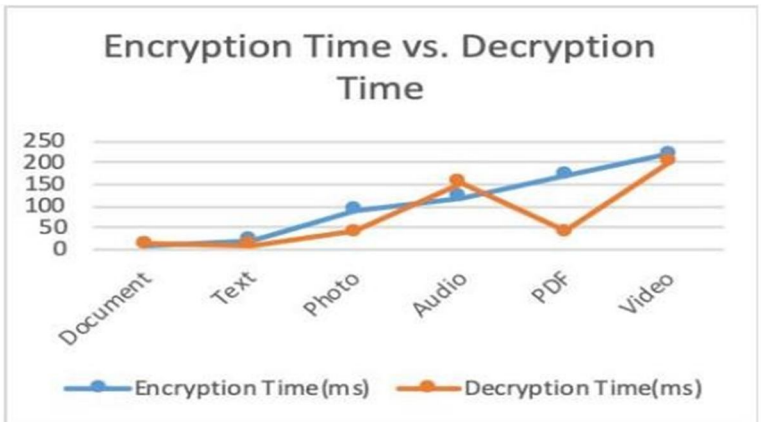
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

3) Time Graph For Proof Of Stack Algorithm



The time graph for the Proof of Stake (PoS) algorithm illustrates the duration taken by the algorithm to process each epoch within a blockchain network. Each epoch represents a predefined period during which validators are selected to validate transactions and create new blocks. The time taken for each epoch, depicted on the y-axis of the graph, reflects the efficiency and performance of the PoS algorithm in processing transactions and achieving consensus. As shown in the graph, the time taken for each epoch may vary over time due to factors such as network congestion, changes in validator participation, and updates to the PoS algorithm itself. Generally, a decreasing trend in the time graph indicates improvements in the efficiency and scalability of the PoS algorithm, resulting in faster transaction processing times and reduced network latency. Conversely, an increasing trend or fluctuations in the time graph may indicate challenges or inefficiencies within the PoS algorithm, such as increased computational requirements for validating transactions or congestion within the network. These fluctuations may prompt network operators to implement optimizations or adjustments to improve the performance and stability of the PoS algorithm.

4) 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.

VI. CONCLUSION AND FUTURE ENHANCEMENT

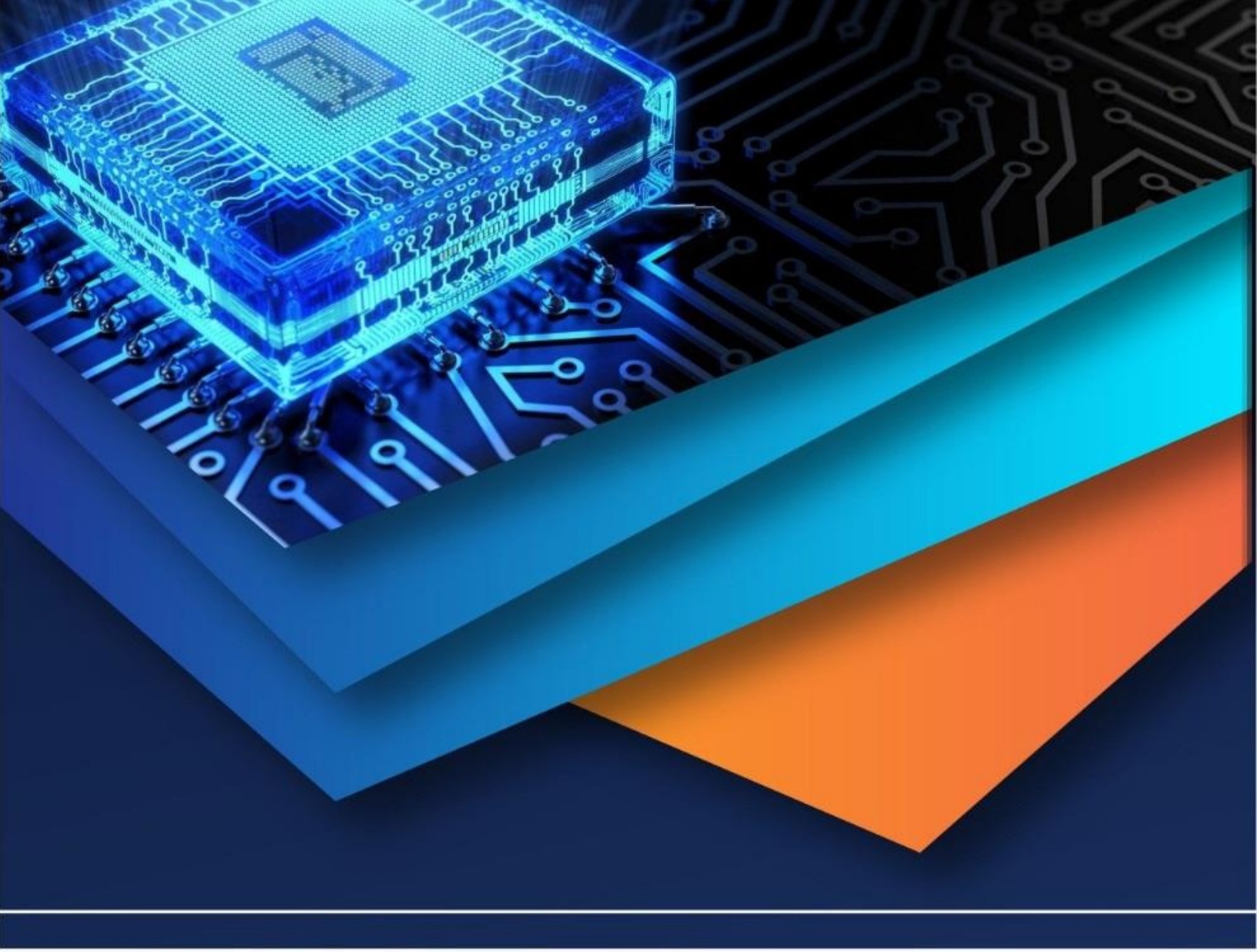
The integration of blockchain technology into forensic investigations represents a significant advancement in digital forensics and evidence management. By leveraging blockchain and smart contracts, this system revolutionizes key forensic processes, enhancing data security, traceability, and operational efficiency. Blockchain's inherent immutability and decentralization provide robust protection against tampering and unauthorized access, while smart contracts automate tasks, reducing errors and expediting investigations. In an era of growing digital evidence complexity, this integration is invaluable for forensic professionals and the criminal justice system, ensuring justice is pursued with utmost security and integrity. This advancement paves the way for a future where forensic investigations are conducted efficiently and securely, maintaining the pursuit of justice amidst evolving challenges.

Future work in this field could focus on enhancing the scalability and interoperability of blockchainbased forensic systems to accommodate larger volumes of digital evidence and facilitate seamless integration with existing forensic tools and databases. Additionally, research efforts could explore the development of advanced analytics and machine learning algorithms tailored for blockchainbased forensic analysis, enabling more effective detection of suspicious activities and patterns within blockchain data.

REFERENCES

[1] IoT Devices Installed Base Worldwide 2015–2025|Statista. Available online:https://www.statista.com/statistics/471264/iotnumber-of-connected-devicesworldwide/ (accessed on 29 December 2022).
[2] Xu, L.; Jurcut, A.D.; Ranaweera, P. Introduction to IoT Security; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]
[3] 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]
[4] 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).
[5] 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]
[6] 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]
[7] 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).
[8] 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]
[9] 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]
[10] 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.
[11] 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.
[12] NSL-KDD|Datasets|Research|Canadian Institute for Cybersecurity|UNB. Available online: https://www.unb.ca/cic/datasets/ nsl.html (accessed on 29 December 2022).
[13] 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.
[14] 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/aboutgovernment/governmentsystem/local-government. Accessed 03 Nov 2022.
[15] Western cape government, "Municipalities in the Western Cape," [Online]. Available: https://www.westerncape.gov.za/ general-publication/municipalities-western-cape. Accessed 03 Nov 2022.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)