International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

PRESERVING INTEGRITY OF FORENSIC EVIDENCE USING BLOCKCHAIN

Vinoth Kumar R [1], Haritha S[2], Sooritha M[3] , Shanmugavaruni S[4]
[1]Assistant professor, Dept. of IT, Rajiv Gandhi College Of Engg. & Tech., Kirumampakkam, Puducherry, India
[2]UG Scholar, Dept. of IT, , Rajiv Gandhi College Of Engg. & Tech., Kirumampakkam, Puducherry, India
[3]UG Scholar, Dept. of IT, , Rajiv Gandhi College Of Engg. & Tech., Kirumampakkam, Puducherry, India
[4]UG Scholar, Dept. of IT, , Rajiv Gandhi College Of Engg. & Tech., Kirumampakkam, Puducherry, India

ABSTRACT
The integration of blockchain technology into forensic investigations presents a transformative approach to addressing critical challenges in legal and criminal justice systems. By utilizing smart contracts—self-executing agreements that follow predefined rules—key processes such as evidence tracking, chain of custody management, and access control can be automated and secured. Smart contracts ensure transparency and integrity in forensic operations by recording all transactions and actions immutably on the blockchain, significantly reducing the possibility of tampering or human error. Blockchain's decentralized structure, cryptographic security, and immutability provide unparalleled protection for sensitive data. Once information is recorded on the blockchain, it becomes virtually unalterable, ensuring the reliability and authenticity of evidence. This feature is vital for maintaining an unforgeable chain of custody and safeguarding the integrity of forensic evidence throughout legal proceedings. Using Remix IDE and Solidity, forensic investigators can develop Ethereum-based smart contracts to manage and store critical data in a tamper-proof manner. Every transaction is time-stamped and securely stored on the Ethereum blockchain, creating an indisputable ledger that strengthens the trustworthiness of investigations. In summary, integrating blockchain into forensic investigations enhances operational efficiency, reduces the likelihood of errors and disputes, and provides a transparent, immutable record of forensic processes. This innovation significantly improves the overall integrity and trust in legal and criminal justice investigations.
Keywords: Ethereum blockchain, Remix IDE, tamper-proof manner.

I.INTRODUCTION:

Forensic intelligence is very critical when it comes to examining cyber attacks or digital crimes as it entails specialized knowledge in collection and evaluation of digital assets. Forensic Investigators conduct their investigations based on methods and principles which aim at securing the integrity of the evidence throughout the investigation. Where there is an ongoing maintenance of the continuity of the evidence, credibility and acceptability of evidence by the court is maintained by creating a transparent and proper legal chain for the preservation of the evidence. The second stage is called the examination stage where the digital information is copied correctly without adjusting the original evidence for further examination. In the subsequent stage, specialists analyze the imaged information to extract the necessary information such as erased documents, schemes of a remote strike, and many others. This phase is aimed at providing recommendations, the determination of the infringer, and the connectors of the legal actions. Such an analysis should however depend on relevant technical capabilities, scrutiny of complexities, and the understanding of spatial

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

considerations in digital forensic techniques. Clients' involvement is a critical part of this stage in order to carry out exhaustive analysis and 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 competitive solution relative to the available ones protects the privacy of users in permissionless blockchains by giving them ownership of their transaction data and reducing the on-chain privacy concerns. Using symmetric cryptography and smart contracts on Ethereum, the system works by allowing data providers to include persons who can be granted an access control list. Later on, the data consumers are allowed to check their approval stub from this approval list to enable them to have access. After such verification has been done, the consumers may wherever possible obtain a security key from the owners of the data in order to have access to the protected material. This procedure is accomplished by executing smart contracts coded in Solidity to allow the safe transfer of keys. These smart contracts are executed on Ropsten test network for measurement of their operations in real time. ***[2]MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture [2]*** The MF Ledger platform aims to provide the interested parties with a trusted, integrated means for conducting digital forensics investigations. However, even before the initiation of any recording to the blockchain ledger, it is clear that the stakeholders enter into exchanges and agreements on some aspects of the investigation. In order to do this blockchain based smart contracts are used to control the resources used during investigations in a secure manner with a sequence of interactions using sequence diagrams. The design of this system model guarantees some strong integrity and protective and preservative measures that are able to ensure that once the evidence is stored that includes the chain of custody only in a private permissioned and encrypted blockchain ledger etc, cascade of evidence does not get altered as the triad of data availability applies in one context. In principle, MF-Ledger increases the security and trust in performing the digital investigations in the context of multimedia whilst addressing threats that will come up in the future. ***[3] Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems [3]*** In this paper, we present a new term and framework-IoT forensic chain (IoTFC), that improves the practice of forensic investigation through the application of blockchain technology, especially in the context of IoT and social environments. Through the use of blockchain's decentralized system, IoTFC is specific in increasing the evidence's credibility and reliability independent of the geographic scope over which investigations may cut across. It does so by creating evidence in such a way that the privacy of the audience is maintained during the review and validation of the evidence meeting all the aspects of its authenticity, immutability, traceability, resiliency, and distributed trust. Furthermore, it contains information about what, how and when evidence was collected, examined and reported which is recorded in the blocks of the core arch of IoTFC facilitating the tracking of provenance of the information. This level of transparency over the evidential chain makes Insedeprint examination results more credible and fosters more confidence in the printed examination combitus_ll the expo_sitors even with examination isolation bicarbonate. Moreover, the paper discusses the use of blockchain as a medium for related secured communication for defense purposes where guaranteed privacy is secured through signing messages using relevant private keys. Quite opposite to this view, the use of blockchain technology has been found to satisfy some of the least requirements in digital forensic processes especially with regards to evidence and its management. [4] **Blockchain based Digital Forensics Investigation Framework [4]** A comprehensive solution has been developed to address the growing threat of digital forensics tampering. This method combines a variety of technologies to protect the integrity and provenance of sensitive digital forensic data. Initially, the forensic data is hashed using the SHA-256 algorithm, which creates an indestructible fingerprint. duplicate for each data The data is then encrypted using the AES Rijndael algorithm, which further

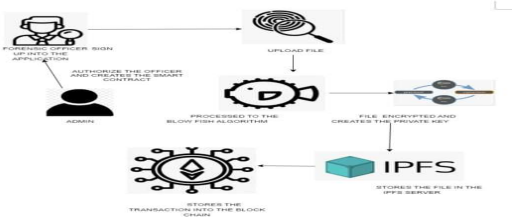
International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

improves security. It then uses blockchain technology to store highly secure and encrypted data. This ensures data is immutable and tamper-resistant. Deployment of this solution is facilitated through a Windows application built in Visual Studio, which acts as both a client and server component. On the server side The AES Rijndael algorithm is used to encrypt forensic data. which are then stored in blockchain blocks. [5] **A blockchain based digital forensics framework for IoT applications [5]** A key feature of the IoF is the use of a blockchain-based case chain to manage the investigation process. Including custody and evidence chain Consensus mechanisms are in place to deal with cross-border legal challenges. Guaranteed transparency and facilitate judicial referrals. The IoF also uses programmable network-based cryptographic primitives to reduce complexity. This is especially beneficial for energy-efficient IoT devices. This increases the novelty of the proposed framework. IoF's Diversified Automated Security Operations Center Cyber Forensic Investigators Various crimes Allows it to be used for Manage self-initiated evidence under chain of custody protocols. The framework guarantees security services as needed. Ensuring the integrity and confidentiality of digital evidence Experimental evaluation and comparison with state-of-the-art frameworks demonstrate the effectiveness of IoF across multiple metrics. including complexity Waste of time Memory and CPU usage, gas usage, and power analysis.

III. PROPOSED SYSTEM:

The proposed system enhances the security of cybercrime investigations by integrating blockchain technology with the Blow fish Algorithm algorithm to protect digital evidence. While blockchain ensures immutability and prevents tampering, it lacks built-in encryption, making stored data vulnerable to unauthorized access. To address this, the system encrypts digital evidence using BF before storing it on the blockchain. This encryption transforms the data into an unreadable format, which can only be deciphered by authorized users possessing the decryption key, thereby maintaining confidentiality even if the blockchain is accessed by attackers. The system leverages Ethereum-based blockchain technology to create a secure, tamper-proof ledger, where each transaction related to the evidence is time-stamped and stored immutably, ensuring data integrity. Remix IDE is used to develop smart contracts in Solidity, which automate critical processes like encryption, storage, and access control, ensuring that predefined rules are followed to enhance transparency and security. These smart contracts are deployed on the Ethereum blockchain, storing every transaction securely and immutably, with timestamps that serve as a record of all activities related to digital evidence. This combination of encryption and blockchain, coupled with smart contracts, offers a comprehensive solution for securing the confidentiality and integrity of digital evidence throughout the investigative process. By integrating encryption, blockchain, and Solidity-based smart contracts, the system creates a more robust foundation for building legal cases and safeguarding justice, while allowing forensic investigators to efficiently manage evidence within a trusted and secure framework.

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

DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

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 BLOW FISH 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:

Data Encryption Module (Blow fish Algorithm)

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, Blow fish Algorithm, 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. Blow fish Algorithm 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

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

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.

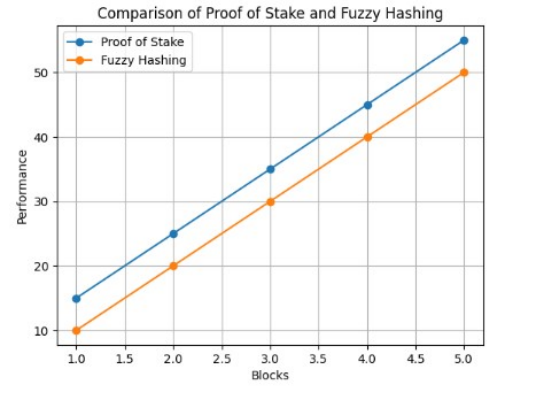
Reporting and Logging Module

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.

COMPARISON OF FUZZY HASH AND PROOF OF STACK ALGORITHM:



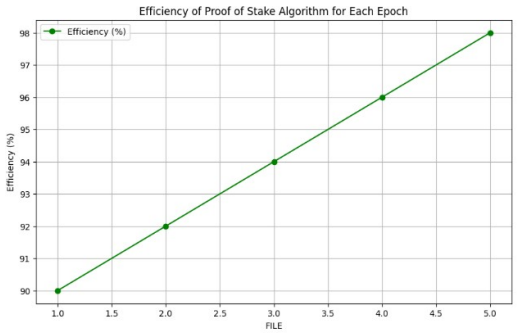
The comparison between Fuzzy Hashing and Proof of Stake (PoS) algorithms involves assessing their respective strengths and weaknesses in different contexts, particularly within the realms of cybersecurity and blockchain technology.

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

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

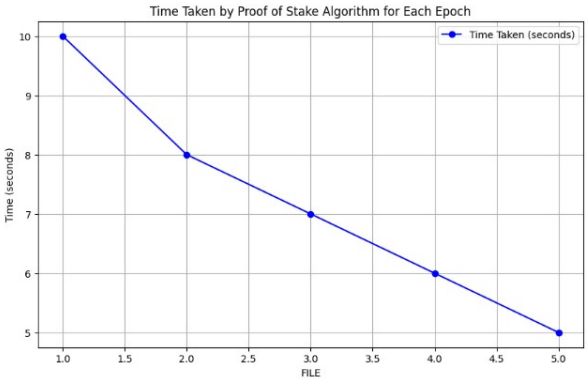
excels in identifying similar or identical files despite alterations, making it invaluable in malware detection, data deduplication, and digital forensics. Fuzzy Hashing's ability to detect similarities within datasets, even with slight modifications, enhances its utility in cybersecurity for identifying 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.

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.

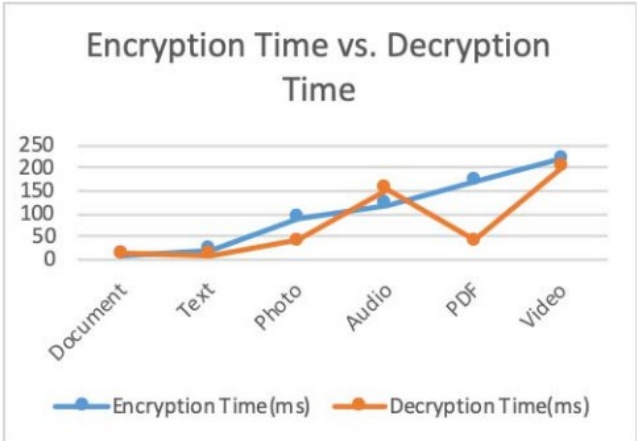
TIME GRAPH FOR PROOF OF STACK ALGORITHM:



International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

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.

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 ENCHANMENT:

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 blockchain-based 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

DOI:10.46647/ijetms.2025.v09i02.114 ISSN: 2581-4621

blockchain-based forensic analysis, enabling more effective detection of suspicious activities and patterns within blockchain data.

REFERENCE:

- 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.