iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71074

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 13 Issue V May 2025- Available at www.ijraset.com

Data Sharing in Cloud Environment through Blockchain and IPFS in Secure Manner

Mrs.S.Sri Sayelakshmi[1], Dr.R.G Suresh Kumar[2], M Harini[3], B Oviya[4]
[1]*Assistantprofessor,* [2]*Head of the Department,* [3, 4]*UG,Dept of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India*

Abstract: ***In modern cloud computing environments,dataisoftenstoredoncloud servers in the form of ciphertext to ensure security and confidentiality. Access to this encrypted data typically requires a third party to provide an access key to the consumer.However,theexistinguseofthe SHA-256 encryption method has limitations, as it leaves the data vulnerable totampering.Toaddressthisissue,aProof of Stake (PoS) algorithm is proposed as a more secure alternative. In this approach, data is encrypted usinga robust encryption algorithm,andalltransactionsarerecorded on a blockchain using the PoS algorithm. This method not only enhances data security by making tampering more difficult but also ensures the integrity of transactions by securely storing them in blocks.Theproposedsystemoffersa more resilient and tamper-resistant solution for cloud data storage and access, managing sensitive information in the cloud. Additionally, it reduces dependency on third-party key providers, further minimizing security risks.***

Keywords: Cloud Security, Proof of Stake (PoS), Blockchain, Data Integrity, Encryption, Tamper-Resistant Storage.

I. INTRODUCTION

With the rapid advancement of cloud computing, secure data sharing has emerged as a critical concern for individuals and businesses alike. Conventional cloud storage systems relyon centralized servers, which pose risks such as hacking, single points of failure, and internal misuse. To tackle these securityvulnerabilities,ablockchain-based hierarchical semi-decentralized model incorporating the InterPlanetary File System(IPFS)isintroducedforsecure and efficient data sharing.In this approach, blockchain acts as the backbone for managing access control, recording immutablepermissionlogs,andpreventing unauthorized modifications. The hierarchical structure facilitates role-based access, making it well-suited for organizations with complex access needs. Additionally, smart contracts automate access control, ensuring security and transparency while reducing dependency on third-party entities.

Meanwhile, IPFS decentralizes data storage by distributing files across a peer- to-peer (P2P) network. Data is hashed and divided into chunks, enhancingredundancy and making it tamper- resistant. Instead of storing entire files on the blockchain, only their corresponding content hashes are recorded, ensuring efficient storage and faster retrieval.

This hybrid semi-decentralized approach balances security with performance. Unlike fully decentralized systems, which may face latency issues, this method enables designated nodes to manage access while maintaining distributed storage. By combining blockchain transparency and IPFS's decentralized framework, this system ensures a scalable, efficient, and secure solution for modern cloud-based data sharing.

A. Interplanetaryfile System (IPFS)

The InterPlanetary File System (IPFS) is a peer-to-peer (P2P) distributed storage protocol designed to offer decentralized, secure, and efficient data management. Unlike traditional cloud storage, which relies on centralizedservers, IPFS divides files into smaller chunks,assignsthemuniquecryptographic hashes, and distributes them across multiple network nodes.When retrieving a file, IPFS locates it using its content hash rather than a fixed server location. This enhances tamper resistance, as any modificationtoafileresultsinanewhash, ensuring data integrity. Moreover, IPFS minimizes bandwidth costs by allowing data to be fetched from the nearest available node, increasing both speed and efficiency.This technology is widely utilized in blockchain-based applications, decentralized apps (dApps), and secure data sharing, offering advantages like redundancy, improved availability, and censorship resistance. By eliminating the reliance on centralized authorities, IPFS provides a scalable andresilient approach to modern data storage.

B. Block Chain

Blockchain is a decentralized, distributed ledger technology that securely records transactions across multiple nodes. Each transaction is stored in a block,which is cryptographically linked to the previous one, forming an unbreakable chain of records. This ensures tamper resistance, as alteringa single block would require modifying all subsequent blocks, making fraudulent changes highly impractical. Unlike traditional centralized systems, blockchain operates on a peer-to- peer (P2P) network, eliminating the need for intermediaries.

Transactions are verified through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), ensuringsecurityandtrust. Blockchainhas applications beyond cryptocurrencies like Bitcoin and Ethereum—it is widely used for smart contracts, supply chain management, and secure data sharing. By offering decentralization, transparency,and security, blockchain enhances data integrity and trust, making it a powerful tool for secure digital transactions across industries.

II. LITERATURE SURVEY

Elias Ribeiro da Silva, Jacob Lohmer, Michelle Rohla, Jannis Angelis [1] explored how blockchain and data sharing enhance circularity in the electric vehicle (EV) battery supply chain by ensuring transparency and traceability. A blockchain-based immutable ledger records the entire lifecycle of a battery, from raw material sourcing to disposal, enabling stakeholders to verify sustainability and regulatory compliance. This technology also supports second-life applications by identifying batteries suitableforreuseorrecycling,contributing to energy storage and waste reduction. By providing reliable data on battery health and composition, blockchain fosters responsible recycling and resource optimization, leading to sustainable innovation and better collaboration among manufacturers and recyclers.

SmitaAthanere,RameshThakur [2] proposed a blockchain-based decentralized system utilizing IPFS (InterPlanetary File System) to enhance data security in data transfers. Centralized storage models are highly vulnerable to cyberattacks, as they rely on single-point data storage, making them prime targetsfor malicious actors. By integrating IPFS withblockchain,thisapproachdividesdata into hash codes that are stored across a distributed network, significantly reducing security risks. To further strengthen security, the system employs data encryption and a two-level key management strategy. Before storage, data is encrypted to ensure confidentiality. The two-levelkeymanagementsystemrestricts unauthorized access, ensuring that only permitted users can retrieve or modifydata. The immutability of blockchain, combined with encryption and advanced key management, creates a highly secure environment for data sharing, preventing unauthorized modifications and reducing breach risks.

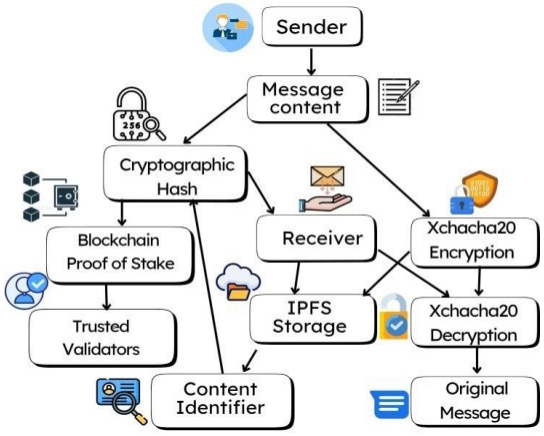
[3] pierpaololoreti,lorenzobracciale,emanueleraso [3] introduced a blockchain-powered smart grid architecture that integrates Secure Multiparty Computation (SMC) and Verifiable Secret Sharing (VSS). SMC allows encrypted computations without revealing private data, while VSSenhances security by splitting encrypted dataacrossmultiplechannels.Thisensures privacy, transparency, and accountabilityin energy data management. Additionally, their multi-channel blockchain structure enhances efficiency for IoT-based smart grids by segmenting transactions, thereby reducing processing loads while maintaining smart contract functionality.

This scalable, secure design ensures decentralized energy management, data integrity, and privacyprotection, makingit ideal for real-world smart gridapplications.

Chaitanya Singh, Deepika Chauhan, Sushama A. Deshmukh, SwatiSudhakarVishnu,RanjanWalia [4]developed Medi-Block, a blockchain- based system designed for secure medical record sharing while ensuring data privacy and accessibility. The system employs bilinear mapping for authentication, eliminating the need for third-party trust authorities and preventing unauthorized access. Medi-Block embeds identity management within the blockchain, reducing single-point vulnerabilities and protecting patient identities. The system also incorporates a two-wayauthentication mechanism between patients and healthcare providers, preventing impersonation. Byremoving intermediaries, Medi-Block improves communication time, reduces operational costs, and enhances security, offering a cost-effective solution for efficient healthcare data management.

YixianZhanga,FengZhaob [5] introduced ECA_MDSS (Efficient Consensus Algorithm for Medical Data Storageand Sharing)toaddressscalability, delay, and throughput challenges in large- scale medical data networks. Their master- slave multi-chain architecture with geographic clustering enhances efficiency and minimizes transmission delays. The system utilizes aggregation signatures to compress transaction data, improving throughput.while a trust modeldynamically evaluates node reliability to mitigate malicious activities. Experimental results showed that ECA_MDSS reduces communication overhead, accelerates consensus, and enhances scalability, making it a secure and efficient solutionfor medical data sharing in modern healthcare environments.

Architecture Diagram Of Proposed System



This diagram represents a decentralized data storage and access system thatintegrates IPFS (InterPlanetary File System) with blockchain technology and cloud storage. In this setup, a Data Owner first uploads their file to a cloud storage server. A unique hash, which is a digital fingerprint of the file, is then generated and uploaded to the blockchain through IPFS, ensuring a secure and decentralized record of the file. An Admin manages the initialization of the system and the process of uploading the hash to the blockchain, allowing the data to be tracked and verified. The blockchain, managed via multiple IPFS stores thesefile hashes in a distributed network, providing enhanced security, dataintegrity, and availability. Data Users who are authorized to access the file can download it from the cloud storage by using the hash, which verifies the file's authenticity through the blockchain. This setup ensures that the data is securely stored and accessed, with the blockchain providing an immutable record, IPFS enabling decentralized storage, and cloud servers offering efficient file retrieval.

III. PROPOSEDSYSTEM

To enhance the security of cloud data storage and access, the proposed system integrates the Proof of Stake (PoS) algorithm with XChaCha20 encryption,offering a more secure alternative to traditional access control mechanisms. Initially, the data undergoes encryption using XChaCha20, a highly secure and efficient stream cipher recognized for its resistance to cryptographic attacks and extended nonce support, ensuring strong confidentiality and data protection. Once encrypted, the data is managed and accessed through a blockchain framework, where every transaction is securely recorded. By employing the PoSalgorithm, the system ensures that only authorized participants with a stake in the network can validate transactions, thereby making unauthorized modifications extremely difficult.

The combination of PoS and blockchain strengthens data integrity and transparency, as all transaction records are securely stored in immutable andverifiable blocks. Since each block is linked through cryptographic hashes, any attempt to alter stored data would require modifying all subsequent blocks, which is computationally infeasible. This decentralized approach removes dependence on central authorities,ensuring that data access andmodifications remain transparent and secure. By integrating PoS-based blockchain security with XChaCha20 encryption, this system delivers a tamper- resistant, scalable, and highly resilient solution for secure cloud data storage and access management.

A. User Authentication & Key Management

This module ensures secure user authenticationandidentitymanagementby eliminating the reliance on traditional third-party key management systems. Instead,blockchain-basedauthenticationis utilized, offering enhanced security and transparency in verifying users. Each user is assigned a cryptographic key pair, generated through secure encryption algorithms,preventingunauthorizedaccess and identity spoofing. Authentication details are permanently recorded on the blockchain, ensuring a tamper-proof audit trail and accountability. By decentralizing key management, the system significantly reduces the risks associated with data breaches and insider threats. Additionally, to enhance security, multi-factor authentication (MFA) can be incorporated, requiring users to pass multipleverification steps before gaining access. This ensures that only authorized individuals can perform transactions and retrieve stored information securely.

B. Data Encryption Using Xchacha20 & Storage

To Protect sensitive information, this module implements XChaCha20 encryption before storing data in the cloud environment. XChaCha20, a highly secure stream cipher, provides robust protection against cryptographic attacks while supportinglongnonces,ensuringenhanced security for cloud-stored data. Encrypted data is distributed across multiple storage nodes, increasing system resilience and reducing the risk of data loss. A secure blockchain-based key management system isusedtoeliminatesinglepointsoffailure, ensuring secure handling of decryption keys. Additionally, hashing techniques suchasSHA-256areappliedtoverifydata integrity, allowing the system to detect unauthorizedmodificationsinstantly.Even if an attacker gains access to the storage infrastructure, encrypted data remains inaccessible without the correctdecryption key, ensuring strong data security and privacy.

C. Pos-Based Blockchain Integration

This module incorporates the Proof of Stake (PoS) consensus mechanism to secure cloud transactions, offering a more efficient alternative to traditional Proof of Work(PoW).UnlikePoW,whichrelieson computational power, PoS selects validators based on their stake in the network, reducing energy consumption while maintaining high security. All data- related transactions, including storage, retrieval, and modifications, are securely recorded on the blockchain ledger, ensuring immutability and transparency. Since PoS operates through validator selection, it makes data tampering highly challenging, as modifications require consensus from multiple validators beforea transaction is confirmed. The decentralized structure of blockchain further enhances redundancy and fault tolerance, significantlyreducingthe riskof dataloss orcorruption.ByleveragingPoS, this module provides a scalable, energy- efficient, and secure approach to clouddata management, ensuring that only trusted participants validate transactions while preventing unauthorized modifications.

D. Access Control & Authorization

This module implements strict access control mechanisms using smart contracts, ensuring that only authorized users can interact with stored data. The system follows a role-based access control (RBAC) model, defining specific permissions for various user roles, including data owners, administrators, and third-party service providers. Smart contracts autonomously verify and enforce access policies, eliminating the need for intermediary oversight, which helps minimize security risks. Every access attempt is permanently recorded on the blockchain, creating a transparent and tamper-proof log that allows for real-time monitoring and auditing. Anyunauthorized access attempts trigger automated alerts, enhancing threat detection and response mechanisms. Additionally, multi-level permission settings allow customized access control, ensuring that sensitive informationremains secure while enabling authorized users to perform necessary operations without compromising system integrity.

E. Data Verification & Integrity Monitoring

To maintain the integrity of stored data, this module continuously verifies its authenticity and detects unauthorized modifications.Everytransaction,including data uploads, edits, and deletions, is recorded immutably on the blockchain, ensuring accountability and traceability. Secure hashing algorithms, such as SHA- 256, generate unique digital fingerprintsfor stored files, enabling instant detection of any tampering. If an inconsistency is identified, an automated alert system notifies stakeholders of the anomaly, allowing for immediate action. Cryptographic proof mechanisms like Merkle Trees enable efficient verification of data integrity during periodic audits. This module ensures long-term data reliability, providing organizations with real-time integrity monitoring and protectionagainstunauthorizedalterations, corruption, or loss of cloud-stored data.

F. Scalability & Performance Optimization

To support large-scale cloud data storage, this module optimizes system performance and ensures scalability. A distributed architecture replicates data across multiple nodes, preventing single points of failure and enhancing system resilience. PoS-based validation mechanisms ensure faster transaction processing with reduced latency compared to traditional consensus models. Load balancing techniques dynamically distribute workloads across storage nodes, preventing bottlenecks and maintaining system efficiency. Furthermore, off-chain storage solutions like the Inter Planetary File System (IPFS) can be integrated to handle large data files efficiently while storing their references securely on the blockchain. This module ensures that the cloud storage system remains scalable,responsive, and capable of handling increasing data volumes without compromising security or performance.

G. Encryption and Decryption Time Formula

In cryptographic algorithms like XChaCha20, the time taken for encryption or decryption generally depends on the input size, key length, and nonce. For a stream cipher like XChaCha20, the encryption and decryption operations are performed in parallel on each byte of data, which makes the process quite efficient.

The time for encryption or decryption T_{enc} can be expressed as:

$$T_{enc} = k \cdot T_{block}$$

Where:

- k = Number of blocks to be processed (which is proportional to the size of the data)
- T_{block} = Time taken to process one block of data (constant for XChaCha20)

Since XChaCha20 processes the data in parallel, the block processing time $T_{block}$is typically very low, and the overall time scales linearly with the data size. For decryption, the process is similar, asstreamcipherswork the samewayforboth encryption and decryption.

H. Security Measurement

Security in cryptographic algorithms can be evaluated using several parameters, such as the resistance to brute force attacks, collision resistance, and entropy. For XChaCha20, a key aspect of security comes from the length of the key and nonce, making it resistant to attacks like nonce reuse or brute-force attempts. A common security measure for stream ciphers is **key strength**, which can be calculated as:

Similarly, collision resistance and entropy are key measures for evaluating security. The higher the entropy of the key and nonce, the more secure the algorithm.

I. Scalability

Scalability in cryptographic systems refers to the ability to handle larger datasets or an increasing number of users while maintaining performance and security. For XChaCha20, scalability is primarily influenced by the ability to process data in parallel, which reduces the time complexity of encrypting large data.

The scalability $S_{scalable}$ can be represented as:

$$S_{scalable} = \frac{T_{enc}}{N_{data}}$$

Where:

- T_{enc} = Total encryption time
- N_{data} = Size of the data being encrypted

For XChaCha20, as the algorithm processes data in parallel, the total time grows linearly with the size of the data, ensuring efficient scalability.

J. Reliability

Reliability in cryptographic algorithms refers to the ability of the algorithm to maintain consistent security andperformanceundervariousoperational conditions, such as changes in input size, network conditions, and key management. Reliability can be measured using error probability and fault tolerance. The probability of a decryption error $\mathbf{P_{error}}$is calculated as:

$$P_{error} = \frac{E_{faults}}{N_{operations}}$$

Where:

- E_{faults} = Number of operations where errors occur
- $N_{operations}$ = Total number of encryption/decryption operations

$$S_{key} = 2^{L_{key}}$$

Where:

- L_{key} = Length of the key in bits (256 bits for XChaCha20)
- The strength would be $S_{key} = 2^{256}$, which is computationally infeasible for brute-force atte

For XChaCha20, its reliability is high because the algorithm uses a well-defined key and nonce structure, ensuring consistent encryption and decryption performance. The useof a256-bit keyalso contributes to low vulnerabilityto failures, while the use of a 192-bit nonce ensures high security against nonce reuse attacks, contributing to overall system reliability.

IV. RESULT AND DISCUSSION

The implementation of blockchain technology has shown remarkable improvements in key aspects such as integrity, security, and transparency of managing data. Blockchain's decentralized and immutable nature ensures that data remains protected from tampering or unauthorized access throughout its lifecycle. This protection is enhanced by the use of smart contracts, which automate essential tasks like tracking the chain of custody, managing data access, and ensuring that predefined rules arefollowed. This automation leads to a more streamlined and transparent workflow, reducing the risk of human error or manipulation. Additionally, blockchain's time-stamping feature records each pieceof data at specific points, ensuring traceability and enabling verification of its status and integrity. The incorporation of encryption algorithms such as XChaCha20 adds an extra layer of security, ensuring that data remains unreadable to unauthorized individuals, even if the blockchain is accessed. This combination of blockchain, encryption, and smart contracts provides a tamper-proof framework for managing and securingdata. Moreover,thedecentralized natureof blockchain means no single entity controls the data, promoting trust among all parties involved. These advancements ultimately lead to greater efficiency, control overdata, and enhanced confidence in digital security and data management systems. Blockchain’s potential in revolutionizing data management is setting the stage for more secure, transparent, and reliable processes.

A. Improved Integrity

Blockchain technology guarantees the immutability of data by leveraging its decentralized and cryptographic structure. Once forensic data is recorded on the blockchain, it becomes permanently embedded in the ledger. This immutability is achieved through a process where each block of data is linked to the previous block via a cryptographic hash.

$$\text{Integrity} = \text{Hash of Data} + \text{Blockchain Hash of Block}$$

Any alteration to a block would require recalculating the hashes of all subsequent blocks and gaining consensus from the majority of the network, which is practically infeasible. As a result, the integrity of forensic data is preserved, ensuringthat it cannot be tamperedwith or deleted after being recorded. This characteristic is vital in forensic investigations, as it provides a trustworthy and transparent mechanism formaintaining the authenticity and reliability of digital evidence, thereby strengthening the legal admissibility of such evidence in court proceedings. The hash of each block is a digital fingerprint of the data it holds. If any evidence is tampered with, the hash value will change, breaking the integrity chain and making tampering easily detectable.

B. Enhanced Security

Security in blockchain-based forensic systems is significantly enhanced by incorporating encryption algorithmslike XChaCha20. This advanced encryption algorithm ensures that digital evidence stored on the blockchain remains secure and inaccessible to unauthorized parties. XChaCha20 provides a high level of cryptographic security by encrypting data before it is written to the blockchain, rendering it unreadable without the corresponding decryption key. Thisensures that even if an attacker gainsaccess to the blockchain, they cannot decipher the stored data. Byencryptingthe evidence,XChaCha20safeguardssensitive information, maintaining confidentiality and protecting the integrity of the investigation process.

$$\text{Encrypted Evidence} = \text{Ciphertext}(\text{Evidence}, \text{Key})$$

This robust encryption mechanism, combined with blockchain's inherent immutability, creates a secure and tamper- proof environment for handling digital forensic evidence, providing investigators withconfidenceinthesecurityandprivacy of the data.

Here, Ciphertext represents the encrypted form of evidence. The key is a secret used to encrypt and decrypt the evidence. This makes sure only authorized users with the decryption key can access the original data.

C. Automation With Smart Contracts

Smart contracts are self-executing agreements embedded within blockchain technologythat automate crucial processes such as chain of custody tracking and access control in forensic investigations. These contracts are programmed with predefined rules and conditions that, once met, trigger automatic execution ofspecific actions without the need for manual intervention. For example, a smart contract can ensure that digital evidence is only accessed by authorized personnel, maintaining strict control over who can view or modify the data.

$$\text{Smart Contract Execution} = f(\text{Conditions, Actions, Parties})$$

Additionally, smart contracts can automatically log every interaction withthe evidence, creating an unalterable audit trail that tracks the chain of custody from collection to presentation in court. This automation not only enhances efficiency but also ensures transparency and accountability, reducing the risk of human error and manipulation while maintaining the integrity of the forensic process. The smart contract function automatically executesdefinedactions(e.g.,recordingan event, giving access) based on the fulfillment of certain conditions, eliminating manual errors and ensuring consistent rule enforcement.

D. Increased Transparency

Blockchain's decentralized structure ensures transparency by allowing every participant in the network to viewthe entire transaction history. Unlike traditional centralized systems, where a single authority controls and manages the data, blockchain distributes the ledger across all nodes in the network. Thismeans that every addition or modification to the blockchain is visible to all participants, fostering a transparent and trustworthy environment.

$$\text{Transparency} = \text{Public Ledger}(\text{Transaction History})$$

Eachtransactionisrecordedinablockand linked to the previous block, creating a chronological and immutable chain. This transparency is particularly valuable in forensic investigations, as it ensures thatall actions related to digital evidence are openly accessible, verifiable, and tamper- proof. By enabling all stakeholders to monitor the handling and movement of evidence, blockchain promotes accountability and reduces the likelihood of fraudulent activities, enhancing the overall integrity of the forensic process.All transactions (evidence additions, updates) are recorded on a public ledger, which is accessible to all authorized entities. This ensures that the entire chain of custody and data flow is visible and verifiable by stakeholders.

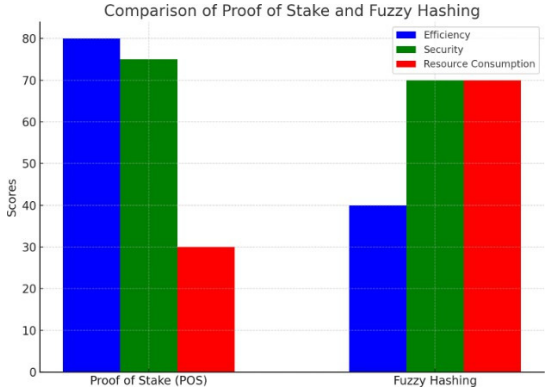
E. Enhanced Traceability

Blockchain records timestamps for every transaction, providing a clear and immutable record of when evidence is recorded,accessed,ormodified.Thistime- stamping feature ensures comprehensive traceabilitybycreatinganauditabletrailof all activities related to digital evidence. Each block in the blockchain contains a precise timestamp that reflects the exact moment a transaction occurs.

$$\text{Traceability} = \text{Evidence Log}(\text{Timestamps, Actions})$$

This allows forensic investigators andlegal professionals to track the chronologicalsequenceofevents,ensuring that the integrity and authenticity of the evidence are maintained throughout the investigation process. The ability to trace every action taken on the evidence enhances accountability and supports the legal chain of custody, making it easier to verify the handling and status of evidence at any given time. This traceability is crucial in legalproceedings, as it provides irrefutable proof of the evidence's history, bolstering confidence in the investigation's findings. In summary, the use of blockchain technology, encryption, smart contracts, and decentralization improves forensic investigations by ensuring data integrity, providing robust security, automating workflows, increasing transparency, and ensuring traceability. These elements combined form a trustworthy, tamper-resistant forensic system.

F. Performance Comparison: Fuzzy Hash vs. POS (Proof of Stake)



This results in faster and more energy-efficient validation. Regarding security, POS ensures safety by incentivizing honest behavior, as participants stand to lose their stakedassets for malicious actions. Fuzzy hashing, however, focuses on detecting similarities and differences between files, ensuring accuracy in identifying tampered data.Whilebothprioritizesecurity,POSis more resource-efficient due to its minimal computational requirements, whereasfuzzy hashing requires significant computational power, especially in large datasets for forensic purposes.

G. Time Encryption And Decryption Time For POS

The encryption and decryption times for POS (timestamp comparison) depend on various factors such as the complexityofthealgorithm,thesizeofthe data being processed, and the specific implementation. In a typical use case, encryption time refers to the time it takestosecurelyencodeatimestamp,ensuringit remains confidential and unaltered. Decryption time, on the other hand, is the time taken to reverse this encoding and retrieve the original timestamp for comparison or processing.

The encryption time $T_{\text{encryption}}$ can be defined as:

$$T_{\text{encryption}} = \frac{S}{P} \times C$$

Where:

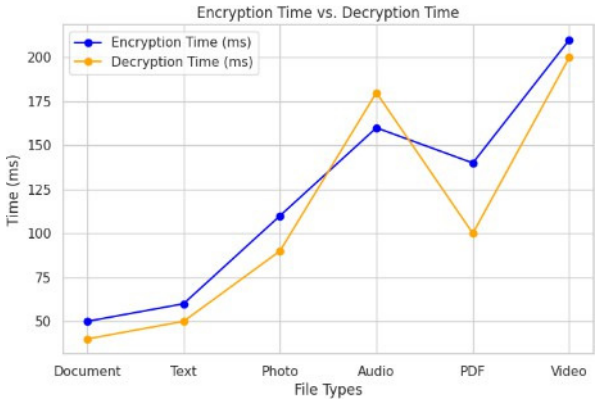
- S = Size of the data (in bytes, for example, the timestamp data).
- P = Processing power (e.g., in terms of CPU cycles per second or encryption rate).
- C = Complexity of the encryption algorithm (which could include factors like the number of rounds or operations in the encryption process).

$$T_{\text{decryption}} = \frac{S}{P} \times C_{\text{decryption}}$$

Where:

- $C_{\text{decryption}}$ = Complexity of the decryption algorithm. In many cases, decryption algorithms are slightly faster than encryption algorithms because they typically involve fewer operations (depending on the encryption scheme).

While POS systems generally do not involve heavy encryption or decryption operations compared to other types of data (such as files or multimedia), these operations can still introduce some delay, especiallywhendealingwithlargedatasets or requiring multiple timestamp verifications. The encryption and decryption times for POS are typically measured in milliseconds, and optimizing the cryptographic algorithms can help reduce these times, improving system



The graph compares encryption time and decryption time for different file types, including Document, Text, Photo, Audio, PDF, and Video. The blue line represents encryption time, while the orange line represents decryption time, both measured in milliseconds (ms). The trend shows that as file complexity and size increase (e.g., moving from text files to video files), both encryption and decryption times increase. However, their behaviors differ slightly at certain points, such as for Audio and PDF files, where decryption takes longer than encryption. The highest processing times occur for Video files, where encryptionand decryption times peak at around 210 ms and 200 ms, respectively. The grid and legend improve readability, making it easier to compare encryption and decryption performance across file types.

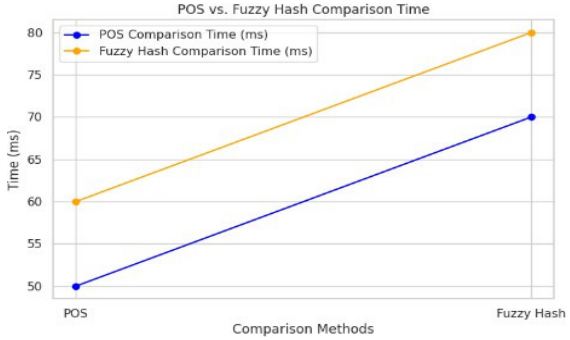
H. Time Comparison Using POS And Fuzzy Hash

Time comparison using Position (POS) and fuzzy hash techniques involves different approaches for evaluating data integrity and identifying changes. ThePOS method compares the exact location of data points, often using timestamps, to assess how closely two sets of data alignor if any modifications have occurred over time. In contrast, fuzzy hashing is used to detect similarities between data that may not be identical but are "close enough" to be considered similar. It works bycreating a hash value that captures the essence of the data while allowing for minor differences (e.g., small edits or changes in encoding).

Fuzzy hashes are particularly useful for detecting subtle modifications in files or data streams, such as file corruption or slight variations, making them more flexible than traditional hashing techniques. By combining both POS and fuzzy hashing, a system can compare the exact timing of data changes while also recognizing data that has been altered in a non-exact way, providing a robust solution for data verification and monitoring over time.

V. CONCLUSION

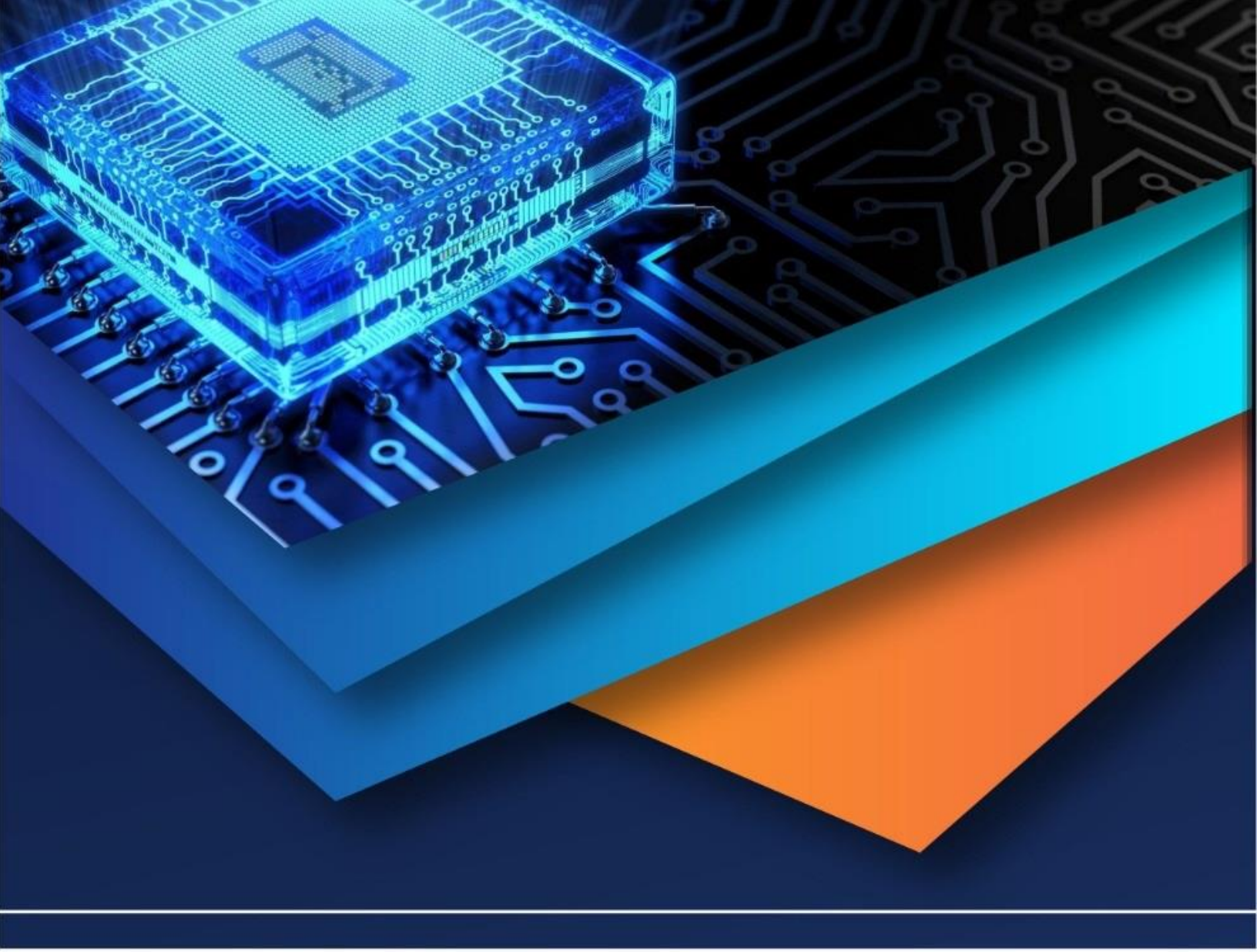
Inconclusion,theintegrationofthe Proof of Stake (PoS) algorithm with XChaCha20 encryption provides a robust and efficient approach to securingsensitive data in cloud environments. By leveragingthehigh-speedperformanceand cryptographic strength of XChaCha20, the system ensures data confidentialitywithout compromising efficiency. Meanwhile,PoS-basedblockchainsecurity enhances data integrity and authentication by recording transactions in an immutable, decentralized ledger, making unauthorized modifications highly impractical. This approach eliminatesrelianceonthird-party key providers, reducing security vulnerabilities and strengthening overall data protection. The combination of PoS and XChaCha20 offers a scalable, verifiable, and tamper-resistant framework, ensuring secure and reliable cloud data management.



Future work can focus on enhancing the system's scalability by integrating sharding techniques in the blockchain to improve transaction efficiency. Additionally, exploring hybrid encryption methods that combine XChaCha20 with post-quantum cryptography can further strengthen security against emerging threats. Implementing AI-driven anomalydetection can enhance real-time threat monitoring, while interoperability with multi-cloud environments can improve adaptability and data redundancy. Lastly, extending the system to support decentralized identity management can provide a more comprehensive security framework.

REFERENCES

[1] Maximilian Wöhrer, Uwe Zdun,— Smart contracts: Security patterns in the ethereum ecosystem and solidity‖, International Workshop on Blockchain OrientedSoftwareEngineering(IWBOSE),IEEE,2018.
[2] Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, —ChainFS: Blockchain- Secured Cloud Storage‖, IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.
[3] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,‖A systematic literature review of blockchain based applications: Current status ,classification and open issues‖ , Elsevier, 2018.
[4] R.Gowthami Saranya, A.Kousalya,‖A comparative analysis of securityalgorithms using cryptographic techniques in cloud computing‖ ,IEEE,2017.
[5] Ilya Sukhodolskiy, Sergey Zapechnikov, —A Blockchain Based Access Control System for CloudStorage,‖ IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
[6] Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare—BlockchainBasedSecureData Storage and Access Control System using Cloud‖ IEEE - ICCUBEA 2019.
[7] Gurudatt Kulkarni, Rani Waghmare, Rajnikant Palwe, Vidya Waykule, Hemant Bankar, Kundlik Koli, —Cloud Storage Architecture‖, IEEE 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2012.
[8] ZhengZhao,SisiDuan, XiaohuiLiang,—A Data Sharing Scheme Based on Blockchain and Interplanetary File System,‖ IEEE Access, vol. 8, pp. 6760– 6771, 2020.
[9] Hsiao-Shan Huang, Hsiang-Yun Liao, Kai-Min Chung, —A Secure File Sharing System Based on IPFS and Blockchain,‖arXiv preprint arXiv:2205.01728, 2022.
[10] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, QiaoyanWen,‖A Survey onthe Security of Blockchain Systems‖,beijing university China, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY