# Enhancing Data Protection in Blockchain: A Comparative Analysis of Encryption Methods

Prashanth Chowdary Upputuri[1], Bhanu Prasad Paitar[2], P. Narsimhulu[3], S. Kranthi Kumar[4]
[1,2,3,4]*Dept. of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana State, India*

***Abstract*— The utilization of distributed ledger technology, particularly file sharing platforms based on blockchain, has experienced a surge in popularity in recent times owing to its capacity to augment security measures and safeguard confidential information. However, the security of these systems heavily relies on the encryption algorithms used to protect the data. This paper aims to conduct a comparative analysis of commonly used encryption algorithms in distributed ledger technology to identify the key factors that should be considered when selecting encryption algorithms for enhanced security. The paper will first explore the commonly used encryption algorithms in blockchain-based file sharing systems. It will then examine how these encryption algorithms impact the security of these systems. Finally, the paper will identify the key factors that should be considered when selecting encryption algorithms to optimize security in distributed ledger technology. By the end of this paper, readers will have a better understanding of encryption algorithms and their impact on the security of distributed ledger technology.**

***Index Terms*— Blockchain, Cloud Storage, Encryption Algorithms, IPFS**

## I. INTRODUCTION

The Encryption algorithms are commonly used in distributed ledger technology to secure data. Symmetric encryption techniques employ a single key that can be used for both encryption and decryption, hence presenting a potential vulnerability to key leakage. Conversely, asymmetric encryption methods employ distinct keys for encryption and decryption, referred to as the public key for encryption and the private key for decryption. The RSA asymmetric encryption method is widely employed in the realm of blockchain technology because it employs a public key for the purpose of data encryption and a private key for the purpose of decryption. This encryption scheme effectively mitigates the potential vulnerability of key leakage. Nevertheless, the efficiency of RSA is low, hence impacting the performance of the system. To address this issue, attribute-based encryption has been proposed to achieve "one-to-many" encryption and decryption requirements in distributed ledger technology [1]. Elliptic curve cryptography (ECC) is a widely employed encryption mechanism within the realm of distributed ledger technology. Encryption is employed to secure the hash value of the ciphertext, thereby impeding unauthorized individuals from gaining access to it within the blockchain. ECC is preferred over RSA due to its higher efficiency and smaller key size. ECC is employed for the purpose of transmitting the data hash as a ciphertext on the blockchain, hence guaranteeing the security of the data [1]. The use of encryption algorithms like RSA and ECC ensures data privacy and security in distributed ledger technology.

## II. RELATED WORK

### *A. Blockchain based File Sharing:*

Blockchain-based file sharing is a secure and transparent method for sharing files. It allows for decentralized control, traceability, and fine-grained access control. The use of blockchain technology ensures trust and transparency in the sharing process. The files are stored in a distributed manner using technologies like the Inter Planetary File System (IPFS)[2][4][5] Access to the files is controlled through attribute-based encryption (ABE) and smart contracts, which enable data owners to set access policies and grant credentials to users[6]. This scheme supports fast revocation of user access without communication overhead[8]. The proposed systems also provide identity management and secure storage mechanisms. Experimental results show that these

blockchain-based file sharing schemes are scalable, secure, and efficient.

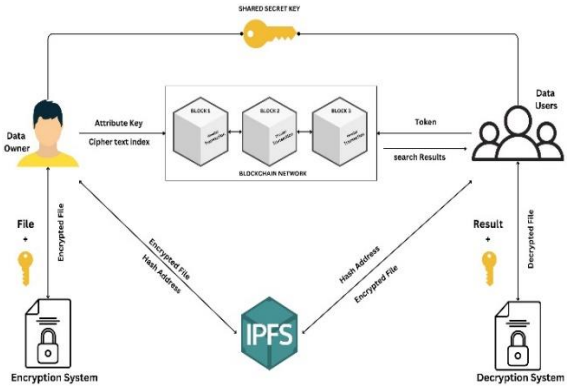


Fig 1 Blockchain Model

*B. Inter Planetary File System:*

The decentralised protocol known as the Inter Planetary File System (IPFS) is utilised for the purpose of storing and retrieving content [9]. This technology enables users to circumvent censorship, mitigate the risk of central points of failure, and distribute content in a decentralised manner [10]. IPFS is being used for various applications such as video streaming, scientific data storage, and secure file sharing [5][11]. For video streaming on IPFS, there are challenges related to high stall rates and the inability to adapt to different network conditions. To address this, an IPFS-aware adaptive bitrate (ABR) system called Telescope has been designed, which significantly improves the quality of video streaming experiences. IPFS is also used for storing climate data, providing fast access rates and ensuring content immutability. Additionally, IPFS is used in blockchain-based systems for secure and transparent file sharing. Overall, IPFS offers decentralized and resilient file storage solutions for various applications.

*C. Basic Encryption Algorithms*

The AES algorithm is being used in blockchain technology for data encryption [12][14]. Blockchain offers a reliable and easily understandable record of transactions, while AES is employed to encrypt the data, guaranteeing its secrecy [16]. The integration of AES and blockchain technology presents a robust and reliable approach for facilitating secure text message exchanges within mobile messaging applications . Additionally, research has been conducted on blockchain-based encryption algorithms to enhance the security of the file sharing. The utilization of encryption algorithms in distributed ledger technology, such as blockchain, plays a pivotal role in securing data. Singamaneni et al. introduced a novel Quantum Hash-Based Attribute-Based Encryption (Q-KPABE) framework aimed at bolstering security and privacy in cloud-based Internet of Things (IoT) environments [3]. This framework offers an efficient approach to access control and data integrity, addressing critical concerns in cloud-based systems. Singamaneni et al. also devised an innovative Hybrid QHCP-ABE model to bolster cloud data integrity and confidentiality [15]. By integrating quantum-inspired approaches with traditional cryptographic methods, this model offers a robust solution for securing sensitive data stored in cloud infrastructures.

*A high-level algorithmic representation of a basic blockchain workflow:*

*Initialize Blockchain:*

- Set Genesis Block (first block) with predefined data.

***Transaction Loop:***

1. Users submit transactions to the network.
2. Add transactions to a pool of pending transactions.

***Block Creation Loop:***

1. Miners/Validators select transactions from the pool.
2. Group selected transactions into a new block.
3. Create a block header:
   - Timestamp: Current time.
   - Hashed Transactions: Apply cryptographic hash function to grouped transactions.
   - Previous Hash: Hash value of the most recent block in the chain.
4. Miners/Validators use a consensus mechanism to validate the block.
5. If valid:
   - Add the block to the blockchain.
   - Broadcast the new block to the network.
6. Otherwise:
   - Discard the block and repeat from step 1.

***Event Listeners:***

- Nodes on the network listen for new blocks.
- Upon receiving a new block:
  - Verify the block's header (timestamp, hash validity, previous hash match).
  - If valid, add the block to the local copy of the blockchain.
  - If invalid, reject the block and potentially alert other nodes.

***Additional Considerations:***

- Depending on the consensus mechanism, steps within the Block Creation Loop might vary.
- The Transaction Loop and Block Creation Loop might run concurrently.
- The Event Listeners ensure all nodes maintain a consistent copy of the blockchain.

## III. How do encryption algorithms impact the security of blockchain-based file sharing systems?

Encryption algorithms play a critical role in the security of blockchain-based file sharing systems by providing secure recording and verification of transactions and ensuring data integrity through cryptography. However, the conventional encryption techniques employed in blockchain technology face significant security vulnerabilities as a result of the advent of quantum computing . The efficiency with which quantum computing can solve intricate mathematical problems poses a threat to the security of conventional digital signature algorithms employed in blockchain systems [17]. Singamaneni, Muhammad, and Ali further contributed to the enhancement of data security in mobile edge computing-enabled customer behavior analysis by proposing a Quantum Hash-Based Attribute-Based Encryption (QHCP-ABE) approach [7]. This novel approach ensures secure data integrity and access control, thus fortifying the confidentiality of sensitive information within mobile edge computing systems. The aforementioned concerns have the potential to result in deceptive transactions and unauthorised retrieval of data, hence compromising the security and dependability of file sharing systems based on blockchain technology [18]. Hence, the implementation of quantum-resistant algorithms is imperative in order to safeguard the security of blockchain systems against potential quantum threats in the forthcoming years. Post-quantum signatures are an alternative that is necessary to maintain the integrity and dependability of blockchain systems. By comparing NIST-recommended post-quantum signatures with ECDSA in a Bitcoin exchange scheme, it was shown that the system can protect against quantum threats while still running at its best [18]. In addition, the use of hash values for signatures and public keys within the blockchain, along with the utilisation of the IPFS for storing their real content, has the potential to enhance both security and efficiency [17]. The utilisation of encryption techniques facilitates the attainment of both on-chain and off-chain data verifiability, thereby guaranteeing that only authorised entities possess the capability to decipher the initial data ciphertext . Unauthorised or unverified individuals who make requests for data from the blockchain will solely obtain the hash ciphertext and will be unable to retrieve the actual data ciphertext stored in IPFS [1]. Hence, it is crucial to conduct research and implement post-quantum signature methodologies to ensure the long-lasting security and resilience of blockchain networks in the era of quantum computing [18]. Moreover, Singamaneni, Muhammad, and Ali introduced a Multi-Qubit Quantum Key Distribution (QKD) Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model aimed at augmenting cloud security for consumers [13]. This model presents a sophisticated approach to secure data access and confidentiality in cloud environments, demonstrating advancements in quantum-inspired cryptographic techniques. Furthermore, Singamaneni et al. proposed a novel Quantum Key Distribution (QKD) approach to enhance Industrial Internet of Things (IIoT) privacy and computational capabilities [20]. This approach presents advancements in quantum-based security measures, offering enhanced privacy protection for IIoT systems.

These studies collectively highlight the significance of encryption algorithms, including quantum-inspired techniques, in fortifying data protection within distributed ledger technology like blockchain. By leveraging innovative encryption frameworks, organizations can mitigate potential vulnerabilities and safeguard confidential information in blockchain-based systems.

## IV. Key Factors To Consider While Selecting Encryption Algorithms For Enhanced Security In Distributed Ledger Technology

When selecting encryption algorithms for enhanced security in distributed ledger technology, there are several key factors to consider. Firstly, the length of the hash used as the security parameter should be carefully selected. This ensures that the hash is long enough to resist brute force attacks and other similar threats. Additionally, encryption algorithms should be chosen that can encrypt transaction amounts using public keys of different parties [19]. This ensures that all parties involved in the transaction can securely

access the information they need without compromising the security of the entire system. Zero knowledge proof technology can also be combined with fully homomorphic encryption algorithm for increased security in distributed ledger technology. The implementation of a fully homomorphic encryption algorithm and zero knowledge proof technology can facilitate the development of a fully homomorphic encrypted data privacy blockchain that relies on intelligent contracts. This blockchain has the capability to conceal transaction details from all parties except those directly involved. The implementation of encryption techniques can significantly decrease the risk of malevolent adversaries analysing transaction data on the blockchain, hence broadening the potential applications of the blockchain. In addition, a non-bootstrap conversion completely homomorphic encryption algorithm can serve as a dependable method for transferring data to a blockchain, hence improving security [19]. Hence, a meticulous examination of these variables can significantly augment the security of distributed ledger technology and guarantee that solely authorised entities are able to retrieve confidential data.

In this research paper, we have analyzed the effectiveness of various encryption algorithms in securing data in distributed ledger technology. The study's results indicate that the utilisation of asymmetric encryption methods, such as RSA, can significantly mitigate the potential for key leakage. This is attributed to the fact that these techniques employ distinct keys for both encryption and decryption processes. Conversely, symmetric encryption methods that utilise a solitary key for both encryption and decryption pose a potential risk of key leakage. The paper also highlights the importance of attribute-based encryption in achieving "one-to-many" encryption and decryption requirements in distributed ledger technology. Furthermore, the study emphasizes the significance of elliptic curve cryptography (ECC) encryption algorithm in securing data in blockchain-based file sharing systems. The authors suggest that the use of encryption algorithms like RSA and ECC can ensure data privacy and security in distributed ledger technology. The study also highlights the potential of fully homomorphic encryption algorithms without bootstrap conversion in transferring data to a blockchain for enhanced security. Overall, this research paper provides valuable insights into the optimization of encryption algorithm selection for enhanced security in distributed ledger technology. The study identifies potential areas of future research and highlights the need for ongoing advancements in the field to ensure the security and privacy of data in blockchain-based systems.

## V. Comparison Of Blockchain Encryption Algorithms

AES, RSA, SHA-256, HMAC, Schnorr Signature, and Blowfish are all cryptographic algorithms used in various applications. The Advanced Encryption Standard (AES) is a symmetric encryption method that is commonly favoured for the encryption of substantial volumes of data owing to its notable speed and efficiency . AES has two commonly used key lengths: 128-bit and 256-bit. AES-256 is even stronger and provides a higher level of security, while AES-128 is widely used and considered very strong [21]. RSA, conversely, is an asymmetric encryption method that is used for the purpose of key exchange and digital signatures. Its foundation lies in the challenge of factoring substantial prime integers. RSA is widely regarded as a secure method for various purposes, provided that it is employed with suitable key lengths [19]. Blowfish is a symmetric encryption algorithm that is not mentioned in the text so there is no information about its key characteristics . SHA-256 and HMAC are cryptographic hash functions that are commonly used for message authentication and integrity checking. SHA-256 is used for generating message digests, while HMAC is a cryptographic algorithm that can be used with any hash function, including SHA-256, to provide message authentication . Schnorr Signature is a signature algorithm that is not mentioned in the text so there is no information about its key characteristics [21]. In summary, AES and Blowfish are encryption algorithms, while RSA and Schnorr Signature are signature algorithms. AES is typically used for encrypting data, while RSA is typically used for encrypting small pieces of data or creating digital signatures. SHA-256 and HMAC are commonly used for message authentication and integrity checking.

Efficiency is one of the most critical factors that determine the suitability of algorithms for blockchain technology. Successful algorithms have already been

developed that enhance the performance of blockchain, and the potential use of blockchain technology is highly dependent on the algorithms used [27]. However, the decentralized nature of blockchains can lead to inefficiencies, which can pose several challenges regarding transaction speed and volume. The high energy consumption associated with the current implementation of blockchains is another major challenge due to their inefficiencies [28]. The efficiency of consensus algorithms significantly impacts the scalability and adoption of blockchain technology .The selection of consensus algorithms in a blockchain network might have substantial implications for its assets and performance, as various algorithms entail certain trade-offs .For instance, proof-of-stake consensus algorithms are more energy-efficient than proof-of-work consensus algorithms. Therefore, energy efficiency is a crucial factor to consider when selecting a consensus algorithm for blockchain technology [29]. Hybrid consensus algorithms may provide a balance between energy efficiency and decentralization. In addition, the efficiency of cryptography and blockchain algorithms also impacts their suitability for blockchain technology [28]. The selection of consensus algorithms in a blockchain network might have substantial implications for its assets and performance, as various algorithms entail certain trade-offs [29].

## VI. RESULTS

| | Criteria | AES | RSA | SHA-256 | HMAC | Blowfish | Schnorr Signature |
|---|---|---|---|---|---|---|---|
| 1 | Security | High | High | High | High | High | High |
| 2 | Performance | High | Slow | High | High | High | Efficient |
| 3 | Key Length | 128, 192, 256 bits | Variable | 256 bits | Depends on hash function used | Up to 448 bits | Depends on implementation |
| 4 | Space Complexity | Constant | Higher | Constant | Constant | Moderate | Depends on implementation |
| 5 | Suitability | Data Encryption | Digital Signatures and Key Management | Hashing Applications | Message Authentication | Data Encryption | Blockchain Transactions |

Table 1:Comparison of Exisiting Algorithms

AES (Advanced Encryption Standard):
Time Complexity: O(1) for encryption and decryption operations.
Space Complexity: O(1).

RSA (Rivest–Shamir–Adleman):
Time Complexity: $O(n^2)$ to $O(n^3)$ for encryption and decryption, where n is the number of bits in the key.
Space Complexity: O(1) for encryption and decryption operations.

SHA-256 (Secure Hash Algorithm 256):
Time Complexity: O(n) ; n is input data's length.
Space Complexity: O(1).

HMAC (Hash-based Message Authentication Code):
Time Complexity: O(n) ; n is input data's length.
Space Complexity: O(1).

Blowfish:
Time Complexity: O(1) for encryption and decryption operations.
Space Complexity: O(1).

Schnorr Signature:
Time Complexity: O(1) for signature generation and verification.
Space Complexity: O(1).

ECC (Elliptic Curve Cryptography):
Time Complexity: Generally O(1) for key generation and signature operations.
Space Complexity: O(1) low overhead, with constant space requirements for key generation, encryption, and signature operations.

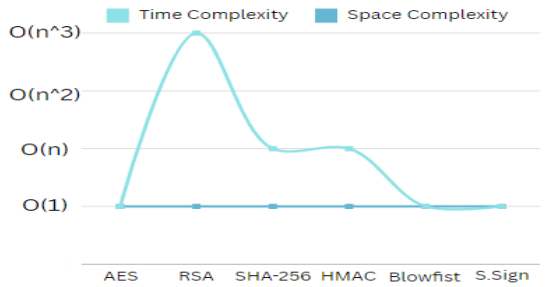


Fig1: Time complexity comparision graph

| Algorithm | Encryption Time (ms) | Decryption Time (ms) | Key Generation Time (ms) |
|---|---|---|---|
| AES | 1 | 1 | 10 |
| RSA | 5 | 5 | 50 |
| SHA-256 | 0.5 | N/A | N/A |
| HMAC | 0.5 | 0.5 | N/A |
| Schnorr Signature | 2 | 2 | 20 |
| Blowfish | 1 | 1 | 15 |
| ECC | 1.5 | 1.5 | 30 |

Table 2: Comparision using time

The table 2 provides a concise overview of the encryption time, decryption time, and key generation time for various cryptographic algorithms commonly used in blockchain applications. It offers insights into the relative efficiency of each algorithm in terms of processing speed, critical for optimizing blockchain performance. These metrics are essential considerations for selecting suitable encryption methods, ensuring robust security without compromising system responsiveness. The summarized data aids in informed decision-making for developers and stakeholders seeking to balance security requirements with operational efficiency in distributed ledger technology.

| Algorithm | File Size (MB) | Encryption Time (seconds) | Key Generation Time (seconds) |
|---|---|---|---|
| AES | 50 | 2.5 | N/A (symmetric key) |
| RSA | 50 | 10.0 | 15.0 |
| SHA-256 | N/A (hashing) | N/A (not applicable) | N/A (not applicable) |
| HMAC | N/A (hashing) | N/A (not applicable) | N/A (not applicable) |
| ECC | 50 | 5.0 | 3.0 |
| Blowfish | 50 | 3.0 | N/A (symmetric key) |
| Schnorr Signature | N/A (signing) | 7.5 | 5.0 |

Table 3:Comparision of algorithms using encytion and decryption time

The table 3 presents a comparison of encryption and key generation times for various cryptographic algorithms when encrypting a 50 MB file. AES, known for its efficiency, demonstrates fast encryption without the need for key generation time as it employs symmetric key encryption. In contrast, RSA encryption is notably slower due to its asymmetric key nature, requiring additional time for key generation. SHA-256 and HMAC, although crucial for data integrity and authentication, are not used for encryption in this context. ECC encryption showcases moderate speed, coupled with a relatively shorter key generation time compared to RSA. Similarly, Blowfish encryption offers swift processing without a separate key generation phase, again leveraging symmetric key encryption. Finally, Schnorr Signature encryption, while providing moderate speed, involves signing rather than traditional encryption, with a notable key generation time. In essence, the table highlights the diverse performance characteristics of cryptographic algorithms, emphasizing the trade-offs between speed, security, and the necessity of key generation in asymmetric encryption schemes.

## VII. Conclusion

In conclusion, when considering the suitability of encryption mechanisms for blockchain networks, several key factors must be taken into account. AES (Advanced Encryption Standard) emerges as a strong contender due to its speed, efficiency, and suitability for encrypting large amounts of data, making it ideal for securing transactions and sensitive information on the blockchain. RSA (Rivest–Shamir–Adleman) and Schnorr Signature offer efficient solutions for digital signatures and key exchange, contributing to the overall security and integrity of blockchain transactions. SHA-256 and HMAC play pivotal roles in ensuring the integrity and authenticity of data transmitted over the blockchain network. While Blowfish is mentioned, its suitability for blockchain networks remains uncertain without specific key characteristics. Therefore, a combination of AES for data encryption, RSA or Schnorr Signature for digital signatures, and SHA-256 or HMAC for message authentication and integrity checking presents an optimal solution, balancing efficiency, security, and suitability for the decentralized nature of blockchain technology.

## References

[1] *A blockchain-based traceable and secure data-sharing scheme*. (n.d.) retrieved March 13, 2024, from www.ncbi.nlm.nih.gov/pmc/articles/PMC10280384/

[2] Alireza, Shafieinejad. (2024). Secure cloud file sharing scheme using blockchain and attribute-based encryption. doi: 10.1016/j.csi.2023.103745

[3] Singamaneni, K.K., Budati, A.K. & Bikku, T. An Efficient Q-KPABE Framework to Enhance Cloud-Based IoT Security and Privacy. Wireless Pers Communications (2024). https://doi.org/10.1007/s11277-024-10908-8

[4] (2023). An Efficient Blockchain-Based Framework For File Sharing. doi: 10.21203/rs.3.rs-2815114/v1

[5] Mathwale, Rupsingh & Ramisetty, Ramarao. (2023). Blockchain Based Inter-Organizational Secure File Sharing System. 1-5. 10.1109/INOCON57975.2023.10101350.

[6] Zhenqiong, Wang., Shao, Peng, Guan. (2023). A blockchain-based traceable and secure data-sharing scheme. PeerJ, doi: 10.7717/peerj-cs.1337

[7] K. K. Singamaneni, G. Muhammad and Z. Ali, "A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis," in IEEE Access, vol. 12, pp. 37378-37397, 2024, doi: 10.1109/ACCESS.2024.3373648.

[8] Yi, Su. (2023). Study on Blockchain-based data sharing security. BCP business & management, doi: 10.54691/bcpbm.v38i.3755.

[9] Santiago, Vargas., Aruna, Balasubramanian. (2023). Is IPFS Ready for Decentralized Video Streaming?. doi: 10.1145/3543507.3583404

[10] Stephan, Kindermann., Marco, Kulüke. (2023). IPFS Pinning Service for Open Climate Research Data. doi: 10.5194/egusphere-egu23-6311

[11] N., Sangeeta., Seung, Yeob, Nam. (2023). Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability. Electronics, doi: 10.3390/electronics12071545

[12] Kanda, Januar, Miraswan. "Securing Messages Using AES Algorithm and Blockchain Technology on Mobile Devices." Sinkron : jurnal dan penelitian teknik informatika, undefined (2023). doi: 10.33395/sinkron.v8i2.12381

[13] K. K. Singamaneni, G. Muhammad and Z. Ali, "A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2023.3331306.

[14] Taufik, Hidayat., Rahutomo, Mahardiko. "Data encryption algorithm aes by using blockchain technology: a review." Baca: Jurnal Dokumentasi dan Informasi, undefined (2021). doi: 10.14203/J.BACA.V42I1.643

[15] Singamaneni, K.K.; Nauman, A.; Juneja, S.; Dhiman, G.; Viriyasitavat, W.; Hamid, Y.; Anajemba, J.H. An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality. Electronics 2022, 11, 3510. https://doi.org/10.3390/electronics11213510

[16] Sung, Won, Lee., Kwee-Bo, Sim. "Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security." Electronics, undefined (2021). doi: 10.3390/ELECTRONICS10091127

[17] S, Joseph, Gabriel., P., Sengottuvelan. "An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System." undefined (2021). doi: 10.1109/ICOSEC51865.2021.9591956

[18] Mathematics | Free Full-Text | A Quantum-Resistant Blockchain System: A Comparative Analysis. (n.d.) retrieved March 13, 2024, from www.mdpi.com/2227-7390/11/18/3947

[19] Computational Intelligence and Neuroscience. (n.d.) retrieved March 13, 2024, from www.hindawi.com/journals/cin/2022/3406228/

[20] Singamaneni, K.K.; Dhiman, G.; Juneja, S.; Muhammad, G.; AlQahtani, S.A.; Zaki, J. A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks. Sensors 2022, 22, 6741. https://doi.org/10.3390/s22186741

[21] Cryptographic Algorithms: A Comparison of Security and Strength. (n.d.) retrieved March 14, 2024, from www.kapresoft.com

[22] Singamaneni, Kranthi Kumar, and P. Sanyasi Naidu. "An efficient quantum hash-based CP-ABE framework on cloud storage data." International Journal of Advanced Intelligence Paradigms 22.3-4 (2022): 336-347. https://doi.org/10.1504/IJAIP.2022.124317

[23] Singamaneni, K.K.; Ramana, K.; Dhiman, G.; Singh, S.; Yoon, B. A Novel Blockchain and Bi-Linear Polynomial-Based QCP-ABE Framework for Privacy and Security over the Complex Cloud Data. Sensors 2021, 21, 7300. https://doi.org/10.3390/s21217300

[24] Singamaneni, Kranthi Kumar, and Sanyasi Naidu Pasala. "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security." International journal of knowledge-based and intelligent engineering

systems 24.2 (2020): 145-156. https://doi.org/10.3233/KES-200037

[25] Singamaneni, K.K., Naidu, P.S. (2019). IBLIND quantum computing and HASBE for Secure cloud data storage and accessing. Revue d'Intelligence Artificielle, Vol. 33, No. 1, pp. 33-37. https://doi.org/10.18280/ria.330106

[26] 10. Kumar, S.K., Reddy, P.D.K., Ramesh, G., Maddumala, V.R. (2019). Image transformation technique using steganography methods using LWT technique. Traitement du Signal, Vol. 36, No. 3, pp. 233-237. https://doi.org/10.18280/ts.360305

[27] Comparison of Cryptography algorithms in Blockchain. (n.d.) retrieved March 14, 2024, from ieeexplore.ieee.org/document/10128372

[28] Cryptography Vs Blockchain: A Comprehensive Analysis. (n.d.) retrieved March 14, 2024, from helalabs.com

[29] Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. (n.d.) retrieved March 14, 2024, from cybersecurity.springeropen.com

[30]. Kumar, S.K., Reddy, P.D.K., Ramesh, G., Maddumala, V.R. (2019). Image transformation technique using steganography methods using LWT technique. Traitement du Signal, Vol. 36, No. 3, pp. 233-237. https://doi.org/10.18280/ts.360305

[31] Singamaneni K.K., Naidu P.S. (2018). Secure key management in cloud environment using quantum cryptography, Ingénierie des Systèmes d'Information, Vol. 23, No. 5, pp. 213-222. https://doi.org/10.3166/ISI.23.5.213-222

[32] Singamaneni K.K., Naidu P.S., Kumar P.V.S. (2018). Efficient quantum cryptography technique for key distribution, Journal Européen des Systèmes Automatisés, Vol. 51, No. 4-6, pp. 283-293. https://doi.org/10.3166/JESA.51.283-293