Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

A Survey on Block Chain Based Big Data Storage Security using Encryption Method

Dr. M.Thangaraj[1], S. Vinodhini[2]

[1]Department of computer science, School of information technology, Madurai kamaraj University
[2]Research scholar, Department of computer science, School of information technology, Madurai kamaraj University

Cite this paper as: Dr. M.Thangaraj, S. Vinodhini, (2025) A Survey on Block Chain Based Big Data Storage Security using Encryption Method. *Journal of Neonatal Surgery*, 14 (32s), 8327-8336.

ABSTRACT
Blockchain-based security practices for bigdataentail block chain technology to store and manage massive amounts of data. It protects data integrity, accessibility and confidentiality by employing cryptographic techniques and decentralized networks. This survey explores the integration of blockchain technology with encryption methods to enhance the security of big data storage systems. As the volume and complexity of data grow, traditional security measures often fall short in addressing the unique challenges posed by big data environments. Blockchain offers a decentralized and immutable framework, ensuring data integrity and transparency. The paper categorizes prevalent encryption techniques, including symmetric and asymmetric encryption, homomorphic encryption, attribute-based encryption, and searchable encryption, evaluating their effectiveness in ensuring data confidentiality, integrity, and accessibility. Furthermore, the survey examines the integration of these encryption methods within cloud infrastructures, highlighting the importance of key management, access control, and compliance with data protection regulations. By synthesizing current research and practical implementations, this study aims to provide insights into the strengths and limitations of various encryption strategies, offering guidance for organizations seeking to enhance the security of their big data storage solutions.

Keywords: *Blockchain,Big dataStorage,Data Security, Encryption Algorithms.*

1. INTRODUCTION

Blockchain-based big data storage security protects massive data repositories by using decentralized, immutable ledger systems that don't depend on centralized authority to guarantee integrity, accessibility and secrecy. The chances of the technology of blockchain are enormousfor improving security in big data storage systems. By ensuring accessibility, confidentiality and data integrity, integrating blockchain technology can enhance this system security. This review examines the issues, future directions, and recommended strategies concerning the security of blockchain-enabled big data storage, as highlighted in recent study and methodologies.

1.1 Block Chain Technology

Since the blockchain-based storage introduction in 2008, blockchain technology, serving as a third-party ledger for transactions, has garnered significant interest. This performs an important part in ensuring the e-commerce security and addressing privacy concerns by acting as a reliable third party. In 2016, over 1 billion dollars was invested in the use of blockchain [1].It offers a plan to handle distributed data interchange, data packet delivery, authentication, and storage in the communication technology [2]. A blockchain network facilitates the sequential assembly of blocks each blocks carries numerous transactions, to collect data. Millions of units can connect and collect data autonomously due to this storage medium, which is essential for unmediated data integration in the Machine to MachineCommunication [3].

Some of the benefits of blockchain technology include agreement protocols, data permanence, distributed control, enhanced protection, and faster transaction processing. Corruption is prevented by its permanent network junctions and digital ledgerof the favourable outcome of transactions depends on agreement amongst key nodes [4]. Web access and private key storage are made possible via decentralization and high security is ensured by complicated algorithms and cryptography. The data block nature is hidden by hashing, rendering irreversible and unchangeable. Transaction validation is accelerated by consensus methods, which identify active nodes. Travellers and overseas workers can transfer money more quickly because of block chain's speedier transaction times than conventional [5].

1.2 Big Data

Big data has gained significant popularity over the past decade, showing a dramatic surge in global data traffic [6]. A new wave of frameworks and innovations is being utilized to effectively handle data, identify key features, and conduct large-

scale analytics.For processing to be done efficiently, major horizontal scaling techniques are needed large, complicated, and challenging to handle with conventional techniques is big data. The data are three divided structures: semi-structured, unstructured, and structured. Big data technologies handle, store, and scrutinize this data. They look for trends in the data to create clever solutions and guarantee effective data management [7].Scientific and engineering departments such as computer vision, IoT data analytics, management of operations and smart city development are investigating big data [8].Big data sets are defined by their volume, velocity, variety, and accuracy. Variety denotes many forms of data, whereas volume indicates the sum of data. Modularity, class imbalance, dimensionality, as well as volatility, data non-linearity and computational accessibility iscertain amount of the difficulties that come with volume. The speed at which data is created is referred to as velocity, and it varies depending on the application. Reliability refers to the correctness and trustworthiness of the data itself because large volumes of data are produced from a variety of sources, including noisy and subpar input information. Big data problems including data provenance, unreliability, and unclean data arranged properly addressed if the standard and coherent precision of data to increase. The big data coherent are to take meaningful insights and patterns out dataset and apply to develop the social and commercial values. Wireless and communication networks, e-health and mobile, smart grids, logistics and transportation are few of the vertical industries in which finds use [9, 10].

1.3 Security storage

Information and communication technology (ICT) resources can be efficiently managed and provided for remote users through cloud storage. It leverages the benefits of virtualization techniques over a massive pool of shared computing resources, including services, processing power, storage and more [11].Datarepository in the sharp-witted world has been transformed by cloud storage, which obviate to have avast storage spaces and build it feasible to manage acquired data effectively. Goodly of collected data are difficult for conventional information systems to retain and manage. Cloud storage is becoming more popular among users of data in smart world as suppliers offer storage options that satisfy a wide range of user needs while cutting costs [12].The blockchain technology constitutes peer-to-peer, decentralized networks which are rapidly improving in terms of security. It leverages hashing algorithms to ensure data security while recording transactions and storing massive volumes of statistics in a single block. Each block has a previous hash and a hash value, and they are all connected [13]. Blocks are validated using the current block's prior hash, which reveals any potentially malicious activity. Consensus algorithms are maintained by blockchain for the repository of delicate data. Nonetheless, big data and cloud systems continue to have difficulties with identification, sharing, storage, and security [14].

2. LITERATURE REVIEW

This section explores current study on blockchain-based Big Data storage security, compiling insights from multiple scholarly works. The table1 lists several study references for Blockchain-Based Big Data Storage Security in many industries, along with their suggested methodologies, goals and study areas.

TABLE 1: SUMMARY OF RELEVANT STUDIES

Ref	Proposed Method	Purpose	Field of this Study	Advantages	Disadvantages
Ghayvat et al., [15]	Healthcare Cloud And Application- Elliptic Curve Cryptographic (HCA-ECC) and Healthcare Cloud And Application- RivestShamirAdvanced Encryption (HCA-RSAE)	**Phase 1:** Establishment of Secure Communication **Phase 2:** Authentication Framework Implementation	Healthcare Informatics	It enhanced healthcare data security and privacy using blockchain. It reduced response time, transaction costs, and improved the resistance.	The complexity of the proposed scheme and high resource demand could limit the scalability in large healthcare systems.
Marichamy and Natarajan[16]	Cryptographic Hash Generator (CHG)-user key creation Discrete Shearlet Transform (DST)-encryption Improved Grey Wolf Optimization Algorithm (IGWO)-	Encrypted BlockchainPlatform for Big Data Management and Exchange of Digital Health Records	Digital Health Records	To improve the safety and confidentiality of medical records through the use of blockchain technology, cryptographic	It might pose some disadvantage in the form of a computational overhead and complexity, limiting

	Verification			hashing,encryption , and optimization techniques to ensure efficiency and faster processing compared to previous methods.	scalability and efficiency in large health care systems.
Chen et al., [17]	Key Encapsulation Mechanism (KEM)	Strengthen blockchain's privacy security for medical data	Medical data storage system	Combine KEM with blockchain for the security of medical data, allows for on-chain operations, and resists block forgery, all while maintaining good throughput performance.	It increased computational complexity due to the combination of symmetric and asymmetric encryption that might affect scalability and efficiency in large-scale medical applications.
Ugochukwu et al., [18]	RSA with the peer-to-peer distributed network powered by Ethereumsmartunion technology	Blockchain ensures the safe and public sharing of consumer data across parties, hence mitigating security and privacy issues in the field of logistics.	Logistic Management	Enhanced logistics management by using blockchain and RSA encryption to improve security, privacy, and efficiency. The system proposed would have higher throughput and lower latency than the existing systems.	The limitation of methodology and lack of reference materials might affect the depth and generalizability of the proposed system.
Sun et al., [19]	Trust paradigm that facilitates multi-CA cohabitation	Function of intelligent big data platforms, benefits of information technology fusion, and assessment model using "Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)" technique	Smart City	Blockchain-based trust model for government data sharing demonstrated it was positive impact in the development of smart city in Hefei as it had improved governance as well as resource efficiency.	The limited generalizability since that was based on empirical analysis from only Hefei. It might not be applicable in other regions that had differences in governance and infrastructure.
Ren et al., [20]	Inter Planetary File System (IPFS), Agricultural Sample Data Chain (ASDC), Ethereum, and Merkle	**Phase 1:** ASDC Consortium Blockchain **Phase 2:** IPFS Network	Agriculture	A new approach based on double blocks using IPFS and Ethereum, which enhanced	The complexity in implementation when consortium

	Patricia Trie (MPT)	Integration **Phase 3:** facilitate communication between the ASDC blockchain and the IPFS network using Oracle Mechanism **Phase 4:** Enhanced MPT Accounts **Phase 5:** Utilization of Ethereum Technology **Phase 6:** Block Hash Creation and Uploading		security, retrieval speed, and the performance of agri-IoT data.	blockchain and IPFS were combined, because that would not solve any scalability problem with the large agri-IoT networks.
Liu and Zhang, [21]	ECC (Ellipse Curve Cryptography)	To enhance IoT data security and storage efficiency with ECC encryption and compressed sensing.	Cryptography	It enhanced IoT security with ECC encryption, in addition to improving storage efficiency with compressed sensing, and it performs better than similar algorithms in these two aspects.	The combination of ECC encryption and compressed sensing might add complexity and computation overhead, which could influence the performance in large-scale IoT systems.
Agrawal et al., [22]	Hybrid Encryption Algorithm (HEA), Fog Computing Model (FCM), Elliptic Curve Diffie-Hellman (ECDH),	A blockchain and fog computing model was to be developed that provides secure access control for data, distributed storage of data, and authentication using a hybrid encryption algorithm for increased security and reliability.	Blockchain, Fog Computing, Data Security, Distributed Networks, Cryptography	It offered secure, reliable, and decentralized data storage with enhanced authentication and data access control through the implementation of blockchain and fog computing, thereby reaching a 95% reliability score.	Integration of blockchain and fog computing might cause increased computational overhead and possible challenges of scalability in large-scale distributed environments.
Guan et al., [23]	Improved ECC and Homomorphic Encryption.	Improve the efficiency and reliability of big data storage in the cloud environment, considering encryption issues, metadata reliability, and fault tolerance.	Big Data Security, Cloud Computing Encryption, Distributed Systems	Boost encryption efficiency by 27.6%, metadata reliability, and fault tolerance using dual-channel storage.	Integration of multiple encryption methods along with coordination mechanisms might introduce increased

					system complexity and overhead.

3. BLOCKCHAIN BASED BIG DATA STORAGE SECURITY

The type of big data blockchain security practices categorizes the level of sensitivity to ensure appropriate encryption methods for safeguarding levels of information. Low-sensitivity data are encrypted by one encryption method only to achieve fundamental protection without significantly degrading the efficiency of computations. In these, symmetric encryption algorithms include AES, DES, Blowfish, and Two fish that provide efficient confidentiality with low computational overheads. A triple encryption layer to highly sensitive data, Triple Data Encryption Schema (TDES) or Triple Information Encryption structure combines the different techniques for providing stronger security against unauthorized access and tampering. The Hybrid Encryption Algorithm that combines AES (ECDSA-ECHD) with AES-ECC is the highest in terms of security but remains resource-efficient for computations. Blockchain technology is essential for safely managing and archiving large amounts of data. It safeguards data integrity, privacy, and availability through distributed ledger systems and advanced cryptographic methods. Moreover, it offers comprehensive evaluations of various encryption schemes to achieve an optimal balance between protection and efficiency across diverse data types.

3.1 SYMMETRIC ENCRYPTION:

The symmetric encryption techniques used include AES, DES, Blowfish, and Two fish for low sensitivity data encryption.

AES:

For encrypting data used for data confidentiality, specifying the number of changes needed to store array in a manner. The first step involves putting the various domain data like banking cloud computing and healthcare data into an array, followed by cipher modifications over a predetermined number of cycles, influenced by key length.AES is one such encryption that assures safe and efficient encryption of sensitive data blocks for storage in blockchain-based big data storage while maintaining confidentiality by ensuring the swift access and retrieval. It is one of the high-performance requirements and can be implemented using less memory, thus appropriate for the large-scale data storage system. Also, AES fits well with blockchain frameworks by making encrypted data more impenetrable and dependable.Modern file systems like BitLocker (Windows), FileVault (macOS), and eCryptfs (Linux) rely on AES for full-disk encryption. It ensures that even if physical access to storage media is obtained, the encrypted files remain inaccessible without the decryption key. [22]

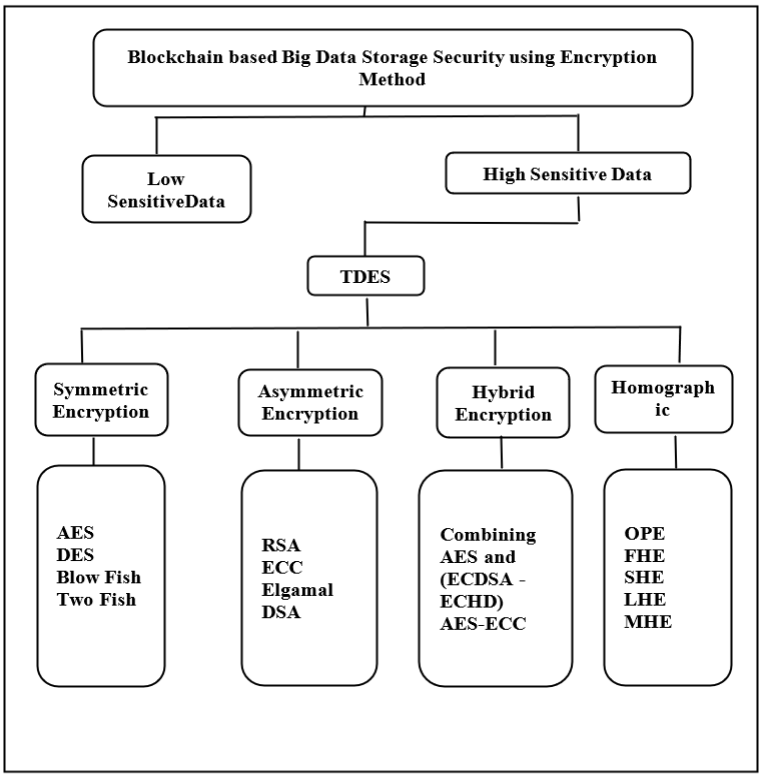

Fig. 1: Big Data Storage Security Encryption Method

DES:

It is a widely used cryptographic technique that can encrypt data in 64-bit blocks and 56-bit keys. However, using a weak key can make susceptible to key assaults. The 56-bit compression secret is utilized by DES after 8 bits from the 64-bit secret are discarded. The medical care, smart home IoTappliances field huge data are securely store in the cloud using this encryption method. For encrypting smaller datasets in the perspective of blockchain-based big data storage security, DES provides a straightforward yet effective method [17].National Institute of Standards and Technology (NIST) officially deprecated DES in 2005 in favor of AES, which offers stronger security and efficiency. DES, however, remains relevant in academic and legacy use cases [40]. DES encrypts data by splitting plaintext into two 32-bit blocks and applying substitution-permutation operations, creating strong diffusion and confusion [18].

BLOWFISH:

Utilizing a block with 64 bits code and a key size differing between 32-448 bits, it is an extremely secure cryptography scheme and has not been found to have any vulnerabilityinbig data encryption in multi-block processing at smart city development and general purpose development in secured big data storage. For security on blockchain-based big data storage, Blowfish is efficient for the encryption of large datasets with low computational overhead. Its flexibility in terms of key size makes it adaptable to many requirements for security but can be less suitable for highly sensitive data as compared to more modern algorithms. Its usage in blockchain environments can complement other encryption techniques for layered security.Blowfish is valued for its speed and efficiency, especially in lightweight cryptographic systems and embedded environments [19].

TWOFISH:

The approach is perfect for embedded hardware and block encrypting and a 256-bit message key, which makes intelligent carts code suitable for CPUs with less power. Encryption speed, key setup procedure, and size of the code are all adjusted to allow for trade-offs. The two-fish algorithm is safe for data exchange even after it has been subjected to several rounds of cryptanalysis attacks without compromising the data in the field of cloud computing and banking data's.Twofish would be suitable for securing large data volumes in decentralized systems at a high level of encryption strength. Its flexibility in size and resistance to cryptanalysis attacks make it a solid candidate for applications requiring high levels of robust and scalable data security in blockchain environments.Two is favored in modern lightweight cryptography for its small memory footprint, fast processing, and flexibility in key size making it suitable for IoT devices [20].

3.2 ASYMMETRIC ENCRYPTION:

RSA, ECC, ElGamal, and DSA are used for protecting medium-sensitivity data while promoting scalability.

RSA:

Identifying and multiplication of two big prime numbers is mathematically straightforward, but factorization is challenging, it is the reason behind the RSA cryptosystem's goal of creating a one-way function that is challenging to reverse. Based on these big prime numbers, the system's public and private keys provide an explanation in mathematics of how cloud computing encryption and decryption work and MultimediaCommunication, handling huge data processing in a secured authentication manner.This allows RSA to be very helpful in securing the key exchange and the transfer of data, because it utilizes asymmetric encryption.[15]

ECC:

ECC is a group of protocols that use discrete logarithm versions for security, similar to number modulo p. They use elliptic curves, numbers related to mathematical objects, which can be added and computed using specific procedures. The premise is discrete logarithms applied to elliptic curves are harder to locate.ECC is one of the most efficient encryption mechanisms that can be implemented in blockchain environments, where low computational overhead is critical. It's the strength of the ability to provide high security, thus being perfect for securing big data storage in blockchain-based IoT and cloud computing resource-constrained environments.

ElGamal:

The secure Elgamal encryption algorithm allows for the division of a single plain text into many cipher texts. Its foundation is the difficulty of sentenceanearlierclarification to the discrete logarithm difficulty in a cyclic group. The encryption procedure requires two exponentiations, whereas the decryption process needs one in smart agriculture .A key power source, an encryption technique, and an algorithm for decryption make up the algorithm.The inherent randomness of the ElGamal encryption algorithm ensures that identical plaintext messages result in distinct ciphertexts, thereby enhancing security in blockchain-based big data storage systems. Its implementation in distributed environments facilitates the secure exchange of data while preserving confidentiality, making it a suitable choice for blockchain platforms where multiple users interact and share sensitive information.ElGamal encryption relies on the computational difficulty of the Discrete Logarithm Problem and provides randomized encryption, in contrast to RSA's predictable approach [16].

DSA:

Asymmetric key algorithms like DSA, which generate digital signatures for user authentication, are used to secure data. Important information is protected and signers are given an individual identity . A message digest is created by the person who sent, who uses a hash function to sign and send. By decrypting the digital signature using the sender's public key, the recipient can confirm the authenticity of both the sender and the message a practice commonly adopted in logistics sectors such as e-commerce and online retail.DSA ensures the integrity and authenticity of stored data so that participants in the decentralized network can verify origin or provenance without dependence on a central authority, hence enhancing data security as well as transparency, primarily where trust and accountability need to be paramount. Reusing the nonce k has led to private key leaks in known attacks such as PlayStation 3's ECDSA vulnerability. Such incidents emphasize the need for robust randomness in digital signatures [20].

3.3 HYBRID ENCRYPTION:

These are combined from RSA-ECC, AES-ECDSA, and AES-ECC, offering high security and computational efficiency.

RSA-ECC:

The hybrid approach is to offer consumers authenticity and data security. This paradigm combines the Secure Hash Algorithm-256 (SHA-256) algorithm for authentication and integrity with various combinations such as AES-RSA and ECC-RSA to provide confidentiality. Because the advantages of both symmetrical and asymmetrical methods are included into the hybrid encrypting method, it has significantly increased the security of the encryption algorithm. One of the strongest hybrid models is the combination of SHA-256 with RSA-ECC. This approach will enhance the confidentiality of data because RSA-ECC integrates the high-speed encryption offered by RSA with the efficiency of ECC in terms of computations and its security. Hybrid technology makes the information quite strong against unauthorized access and tampering, crucial for keeping blockchain data integrity and confidentiality [22].

AES and (ECDSA – ECDH):

AES, ECDSA and ECDH together to provide hybrid encryption offer a safe way to send data. It emphasizes key exchange, integrity, and secrecy. ECDSA creates a digital signature for data, whereas ECDH creates a shared secret key between participants. Symmetric encryption is accomplished by AES by using a single key for both encrypt and decrypt. After the password-protected information and digital signature are transferred across the channel, the recipient uses their public key to verify the digital signature. ECDH offers unparalleled forward confidentiality. AES with ECDSA and ECDH provides the benefits of confidentiality and authenticity of data and ensures forward secrecy, which is a must in decentralized networks to secure data. Thus, the hybrid approach of AES together with ECDSA and ECDH can mitigate risks in a blockchain environment, where even after compromising the private key of an attacker, the communications made previously are safe, and AES is also a good fit to encrypt high volumes of data usually required in storage solutions of block chains[20]. **AES-ECC:**

Integrating asymmetric ECC to securely exchange symmetric session keys with symmetric AES for high-speed data encryption leads to an efficient ECC-based hardware architecture tailored for encrypting medical images. The time complexity is decreased by employing just two multipliers in the development of thePoint Doubling (PD) and Point Addition (PA) blocksused in the medical care big data process. Hybrid encryption utilizing AES and ECC ensures both secure key negotiation and efficient data protection. ECC strengthens cryptographic security by facilitating a robust session key exchange, while AES accelerates the encryption process for large-scale datasets. This dual approach is particularly beneficial in blockchain environments where handling sensitive information demands both high performance and stringent security. The integration of ECC with AES boosts the throughput and scalability of blockchain systems without undermining their cryptographic integrity [15].

3.4 HOMOMORPHIC ENCRYPTION:

These model like Fully Homomorphic Encryption (FHE), Levelled Homomorphic Encryption (LHE), Multiparty Homomorphic Encryption (MHE), and Order-Preserving Encryption (OPE), which allow operations on encrypted data, ensuring privacy in highly sensitive transactions.

Order-preserving encryption (OPE):

OPE is crucial to the security of databases that are exported. OPE plans can be Autonomous or The stateless series. OPE offers the highest level of security that authorized networks can achieve. OPE enables searching and sorting of encrypted data without decryption, ensuring sensitive information is not compromised. This approach proves beneficial in blockchain use-cases where fast data retrieval is important, while strong security mechanisms are necessary to ensure data integrity. Maintaining order improves the flexibility and usability of encrypted data in blockchain environments.When encryption must preserve properties such as order, traditional encryption methods become unsuitable. This limitation has led to the development of Order-Preserving Encryption (OPE), which enables sorting and comparison of ciphertexts without decrypting them. OPE is particularly useful in secure database systems and cloud computing environments that require

operations like range queries on encrypted data[16].

Fully Homomorphic Encryption (FHE):

Completely homomorphic encryption protocol the encryption scheme E is F-homomorphicthat the (efficiently computable) functions are included in the scheme, and the cipher texts are compact. FHE allows computations to be executed directly on encrypted data, preserving confidentiality at every stage of the processing cycle. This facilitates secure data analytics and query operations in a blockchain ecosystem, which is crucial for industries that demand data confidentiality, such as healthcare or finance. The ability to maintain encryption during processing further improves the overall security of blockchain networks, making it perfect for large-scale decentralized applications.Hybrid encryption merges public-key and secret-key cryptographic techniques to achieve both secure key distribution and high-performance data protection. In this method, a session key is secured using an asymmetric algorithm (e.g., RSA or ECC), while the actual data is encrypted with a symmetric cipher such as AES or ChaCha20 [17].

Somewhat Homomorphic Encryption (SHE):

A somewhat homomorphic encryption (SHE) scheme is one that is "F-homomorphic" for a restricted class F. For example, it can evaluate "low-degree" multivariate polynomials homomorphically. The compactness of cipher texts can be broken in a SHE scheme in L-leveled schemes. SHE enables a restricted set of operations on encrypted data, striking a balance between strong data protection and computational feasibility. This makes it ideal for use cases that involve limited encrypted computations, such as executing simple financial operations or performing lightweight data queries in blockchain ecosystems, thereby improving security without compromising system efficiency.This method is commonly implemented in practical systems because it offers a good trade-off between security and efficiency. TLS, the foundation of HTTPS, employs RSA or ECDH for secure key negotiation, and utilizes AES or ChaCha20 for high-speed symmetric encryption of session content [19].

Leveled Homomorphic Encryption (LHE):

The leveled homomorphic scheme is a technique that makes easier to evaluate certain intensity circuits.Legitimately speaking, it is compact and “F-homomorphic”, where the restriction over the length of the cipher text is independent of the degree and F is a collection of every function of a specific degree.This kind of method treats the depth as a configuration parameter that can take on any value. Importantly, if the level is restricted to the highest possible value of L, the model is referred to an L-Leveled homomorphic system. Be aware that plans with L levels could not be compact. LHE brings the ability to perform any kind of computation on any encrypted data at a satisfactory depth, which balances depth with security and efficiency in the computations. This technique is much more useful in the blockchain network that operates in distributed networks as it allows people to do data processing without uncovering the underlying information because of data privacy and data integrity [22].

Multiparty Homomorphic Encryption (MHE):

MHE's minimal communication requirements and versatility make it a promising generic secure multiparty computation (MPC) solution. By permitting multiple parties to collaboratively compute functions on encrypted inputs without disclosing the inputs or results, multiparty homomorphic encryption facilitates collaborative computation while maintaining privacy. MHE increases privacy and security when sharing data with multiple stakeholders. Enabling the collaborative processing of data without exposing sensitive information, MHE safeguards privacy by leveraging blockchain's decentralized architecture, which reinforces data integrity and confidentiality in collaborative environments, thereby enhancing the overall security of blockchain-based storage systems.The MHE is an enhanced form of homomorphic encryption (HE) that combines the principles of secure multiparty computation (MPC) with HE. It enables several entities to collaboratively evaluate a function over their confidential datasets without disclosing their individual inputs [21]. The primary objective of MHE is to facilitate joint data analysis across distinct organizations or legal jurisdictions, while maintaining data privacy, compliance with data protection regulations, and confidentiality safeguards.

4. CONCLUSION

In conclusion, this survey underscores the potential of integrating blockchain technology with advanced encryption methods to fortify big data storage systems against evolving security threats. By evaluating a range of encryption techniques and their deployment within cloud infrastructures, the study highlights critical considerations such as key management, access control, and regulatory compliance. Future research should focus on developing scalable, energy-efficient blockchain-encryption frameworks, exploring interoperability across heterogeneous data environments, and assessing real-world performance through longitudinal case studies. Such efforts will be instrumental in guiding organizations toward robust, adaptive, and regulation-compliant data security architectures. Future research should focus on optimizing these integration models, enhancing interoperability with existing cloud infrastructures, and developing quantum-resistant cryptographic protocols to ensure long-term data security. By addressing these challenges, organizations can leverage blockchain-based encryption frameworks to achieve a higher level of security and trust in their big data storage solutions.

REFERENCES

[1] Gad, A. G., Mosa, D. T., Abualigah, L., &Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. Journal of King Saud University-Computer and Information Sciences, 34(9), 6719-6742. https://doi.org/10.1016/j.jksuci.2022.03.007

[2] Zhang, J. (2020). Interaction design study based on large data rule mining and blockchain communication technology. Soft Computing, 24(21), 16593-16604. https://doi.org/10.1007/s00500-020-04962-0

[3] Aliahmadi, A., Nozari, H., &Ghahremani-Nahr, J. (2022). A framework for IoT and blockchain-based marketing systems with an emphasis on big data analysis. International Journal of Innovation in Marketing Elements, 2(1), 25-34.https://doi.org/10.59615/ijime.2.1.25

[4] Yadav, A. S., Singh, N., &Kushwaha, D. S. (2023). Evolution of Blockchain and consensus mechanisms & its real-world applications. Multimedia Tools and Applications, 82(22), 34363-34408. https://doi.org/10.1007/s11042-023-14624-6

[5] Politou, E., Casino, F., Alepis, E., &Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972-1986. https://doi.org/10.1109/TETC.2019.2949510

[6] Iqbal, R., Doctor, F., More, B., Mahmud, S., &Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. Technological Forecasting and Social Change, 153, 119253. https://doi.org/10.1016/j.techfore.2018.03.024

[7] Surbakti, F. P. S., Wang, W., Indulska, M., &Sadiq, S. (2020). Factors influencing effective use of big data: A study framework. Information & Management, 57(1), 103146. https://doi.org/10.1016/j.im.2019.02.001

[8] Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., &Rokhani, F. Z. (2021). IoT and big data applications in smart cities: recent advances, challenges, and critical issues. IEEE Access, 9, 55465-55484. https://doi.org/10.1109/ACCESS.2021.3070905

[9] Safhi, H. M., Frikh, B., &Ouhbi, B. (2019). Assessing the reliability of the big data knowledge discovery process. Procedia computer science, 148, 30-36. https://doi.org/10.1016/j.procs.2019.01.005

[10] Renugadevi, N., Saravanan, S., &Sudha, C. N. (2023). Revolution of Smart Healthcare Materials in Big Data Analytics. Materials Today: Proceedings, 81, 834-841. https://doi.org/10.1016/j.matpr.2021.04.256

[11] Li, J., Wu, J., Jiang, G., &Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. Information Processing & Management, 57(6), 102382.https://doi.org/10.1016/j.ipm.2020.102382

[12] Ren, Y., Leng, Y., Qi, J., Sharma, P. K., Wang, J., Almakhadmeh, Z., &Tolba, A. (2021). Multiple cloud storage mechanisms based on blockchain in smart homes. Future Generation Computer Systems, 115, 304-313. https://doi.org/10.1016/j.future.2020.09.019

[13] Manikandan, D., Valliyammai, C., &Karthika, R. N. (2020). Blockchain-based secure big data storage on the cloud. Int J Recent TechnolEngg, 9(4), 37-45. https://doi.org/10.35940/ijrte.D4744.119420

[14] Zhu, Z., Qi, G., Zheng, M., Sun, J., & Chai, Y. (2020). Blockchain-based consensus checking in decentralized cloud storage. Simulation Modelling Practice and Theory, 102, 101987. https://doi.org/10.1016/j.simpat.2019.101987

[15] Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2021). CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. IEEE Journal of Biomedical and Health Informatics, 26(5), 1937-1948. https://doi.org/10.1109/JBHI.2021.3097237

[16] Marichamy, V. S., & Natarajan, V. (2023). Blockchain-based securing medical records in big data analytics. Data & Knowledge Engineering, 144, 102122. https://doi.org/10.1016/j.datak.2022.102122

[17] Chen, Y., Luo, H., &Bian, Q. (2021, October). A privacy protection method based on Key encapsulation mechanism in medical blockchain. In 2021 IEEE 21st International Conference on Communication Technology (ICCT) (pp. 295-300). IEEE.https://doi.org/10.1109/ICCT52962.2021.9658006

[18] Ugochukwu, N. A., Goyal, S. B., Rajawat, A. S., Islam, S. M., He, J., & Aslam, M. (2022). An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method. Mathematics, 10(24), 4670. https://doi.org/10.3390/math10244670

[19] Sun, M., & Zhang, J. (2020). Study on the application of blockchain big data platform in the construction of new smart city for low carbon emission and green environment. Computer Communications, 149, 332-342. https://doi.org/10.1016/j.comcom.2019.10.031

[20] Ren, W., Wan, X., &Gan, P. (2021). A double-blockchain solution for agricultural sampled data security in

Internet of Things network. Future Generation Computer Systems, 117, 453-461. https://doi.org/10.1016/j.future.2020.12.007

[21] Liu, Y., & Zhang, S. (2020). Information security and storage of the Internet of Things based on blockchains. Future Generation Computer Systems, 106, 296-303.https://doi.org/10.1016/j.future.2020.01.023

[22] Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using a hybrid encryption algorithm. Cluster Computing, 1-16. https://doi.org/10.1007/s10586-024-04411-9.