Indonesian Journal of Electrical Engineering and Computer Science
Vol. 40, No. 2, November 2025, pp. 780~788
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v40.i2.pp780-788

Hash-based message authentication code with secure hash algorithm-256 for efficient data sharing in blockchain

Naveenkumar Lingaraju, Manjula Haladappa Sunkadakatte
Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bengaluru, India

Article Info

Article history:

Received Sep 3, 2024
Revised Jul 10, 2025
Accepted Oct 14, 2025

Keywords:

Blockchain
Hash value
Hash-based message authentication code
Secret key
Secure hash algorithm

ABSTRACT

Recently, cloud servers have increasingly been utilized for storing a large amount of data, which is stored in the form of ciphertext. In a decentralised system, the communication overhead on the network is recognized as the main problem due to the numerous transaction data recorded across the data Sharding and nodes with authorized users. Hash-Based Message Authentication Code with Secure Hash Algorithm-256-bit (HMAC-SHA-256 bit) is proposed for secure and effective data sharing in blockchain to overcome this issue. The secure algorithm HMAC serves for authenticating both the data origin and integrity. That uses a cryptographic hash procedure in combination with a confidential key to validate both the verification and tamper-proof content of a message. HMAC consists of a particular content and an authentication key with a hashing code value. In the Blockchain framework, the HMAC algorithm is utilized with the SHA-256bits to generate and validate the signatures of many transactions. SHA-256 is a hash algorithm that creates a 256-bit cryptographic checksum. The blockchain uses HMAC along with SHA-256bits, which is a safe and clearly expressed algorithm to allocate or convey the data securely. The Authentication of HMAC-SHA-256bits achieves the optimal retrieval times of 0.4s, 1.0s, 1.5s, 1.9s, 2.2s, and 2.8s for file sizes of 50KB, 100KB, 150KB, 200KB, 250KB, and 300KB, correspondingly, when compared to interplanetary file system (IPFS).

Corresponding Author:

Naveenkumar Lingaraju
Department of Computer Science and Engineering
University of Visvesvaraya College of Engineering
Bengaluru, India
Email: naveengowdakns@gmail.com

1. INTRODUCTION

The Application of network-based digital technologies has developed in the current era, in that cloud-based storage (CBS) has been identified as a potential framework that helps to manage the expansion of digital data transfer [1]. CBS is a significant emerging development in cloud computing, which offers efficient, effective data management solutions in multimedia data [2]. Cloud storage technology is faced with challenges such as availability, security, storage resource limitations, minimal consistency, poor scalability performance, high cost, and lack of interoperability [3]-[5]. These service providers are particularly unreliable because they are sensitive to attack from external cyber attackers, otherwise even interrupted by their Employees [6]. Essentially, this enables improved data confidentiality risks utilizing whichever cloud-based data transmission protocol. Encryption techniques is a critical security feature for securing data access rights [7], [8]. However, blockchain is a network system that ensures data is secure from various computers that are also called nodes [9]-[11]. The development and integration of blockchain technology in cloud

storage take an approach to address the issues of availability and security in cloud storage [12]. Cloud storage data is suitable for human life; however it has some privacy and security issues [13]. There has been a proliferation of message shielded like meeting records, courtroom evidence, military command instructions, communication records, educational platforms, health systems, business strategy, and other private information like national and corporate confidentiality and individual privacy, which require robust security measures to protect against unauthorized access and ensure data integrity [14]-[16]. The established multimedia data management tools are insufficient to handle exponentially growing data volumes, which leads to enhanced issues with data storage and privacy sharing [17]. The major issue is that users lack control over storage data, which compromises its security when unauthorized attackers have access to speech and cloud data [18], [19]. By focusing on effective data sharing, this research leads to scalable blockchain solutions that are suitable for real-time applications such as secure data sharing [20]. Themost of the traditional data-sharing methods demand on offline transmission that lacks practicality and prone to significant issues like data loss [21]. Furthermore, the risk of privacy breaches based on internet of things (IoT) leads to dissuade individuals from participate in IoT data. While the IoT based data collection majorly improves the decision-making thereby ensuring security and privacy in entire process are essential [22].

Jayabalan and Jeyanthi [23] implemented a elastic blockchain framework through Off-Chain-IPFS for data privacy and security. The symmetric key encryption was utilized earlier then data storing in IPF System model for data cryptographic transformation, and a dual-key encryption scheme served as utilized to pass on the single-key encryption for producing secure key encapsulation to approved entities. The electronic signature enables the transaction into valid and authorized access nodes, and hashing was done through the SHA-256 algorithm. However, it suffered from scalability and indeterminate key management for access control policies due to the utilization of searchable encryption algorithms. Wang and Guan [24] introduced a blockchain-based traceable and secure data-sharing approach. A secure data storage approach was developed which integrates off and on-chain association. The developed model was stored, sharing data records on blockchain and shows as visual representation to recognize the tracking requirement of data parties. However, the model focused on single-point failure which is inherent in the centralized system due to the classical access control solution. Liu *et al.* [25] suggested a multi-authority attribute-driven access control management in blockchain framework for allocation of data communication. The blockchain kept cryptographic transformation data to obtain detailed with flexible permission control authorization. A protocol designed for secure key creation was used in secret key production to realize the secure distribution of key users through an attribute authority. However, the communication overhead on the network is recognized as the main problem due to the numerous data backups and the data spread across multiple nodes that can only be retrieved by users who have been both authenticated and authorized.

Gao *et al.* [26] presented a blockchain with Hierarchical blockchain resource scheduling for an optimized data confidentiality and protection system. Monitoring past work helps to manage peer container status and system resources, which enables to handling of additional tasks and accessible sources among associated infrastructure nodes. However, the model suffered from load-handling limitations because the total number of networking hosts and end-users grew which resulting in less performance. Ugochukwu *et al.* [27] implemented a secure and effective distribution storage model using IPFS in blockchain. The model resolved the logistic system privacy, interoperability, and security challenges, and it generates logistic recommendations to adopt blockchain. However, the integration of various blockchain networks was challenging because of the interoperability issue. From the analysis, the existing model has limitations, such as it suffers from scalability and indeterminate key management for access control policies due to the utilization of a searchable encryption algorithm. It focused on single-point failure, which is inherent in the centralized system due to the classical access control solution. The communication overhead on the network is recognized as the main problem due to the numerous data backups and the data spread across multiple nodes that can only be retrieved by users who have been both authenticated and authorized.

It suffered from load-handling limitations because the total number of networking hosts and end-users grew which resulting in less performance. The integration of various blockchain networks was challenging because of the interoperability issue. The contribution of this research is summarized as follows:

- HMAC is a secure algorithmic user verification system in which a cryptographic secure hashing mechanism is applied mutually along with a symmetric key to determine both the authenticity and integrity of the data block. HMAC consists of a particular data block and a symmetric key with a secure hash code.
- In blockchain technology, the HMAC system applies SHA-256 as its method for authenticating messages securely. To generate and authenticate the signatures of numerous transactions. SHA-256 is a hash algorithm that creates a fixed-length 256-bit hash. The blockchain uses HMAC, which implements SHA-256 hashing algorithm, it is a very confidential and brief approaches to allocate convey data.

The research paper is organized as follows: Section 2 describes the research method for efficient data sharing in blockchain; Section 3 shows results and discussion in terms of quantitative and qualitative analysis and comparative analysis; the conclusion with future work of this research is given in Section 4.

2. RESERCH METHOD

In a decentralized system, the network communication overhead is recognized as the main problem. A semi-decentralized approach is provided with the aim of reducing communication overhead caused by authorized users replicating information on distributed nodes is used in which HMAC-SHA-256 is utilized on the blockchain. The designed HMAC-SHA-256 is justified based on its capability to address challenges in secure data sharing in blockchain. The existing methods are suffered fromindeterminate key management and scalability issues thereby leading to communication overhead. HMAC-SHA-256 integrates cryptographic hash function with secret key that ensures both integrity and authenticity of messages. Figure 1 depicts the semi-decentralized system model. Initially, the data owner encrypts the data and uploads it to a cloud server while the blockchain generates hash code for encrypted data. The hierarchical structure is formed on blockchain in that domain authority is formed by its distributed user.

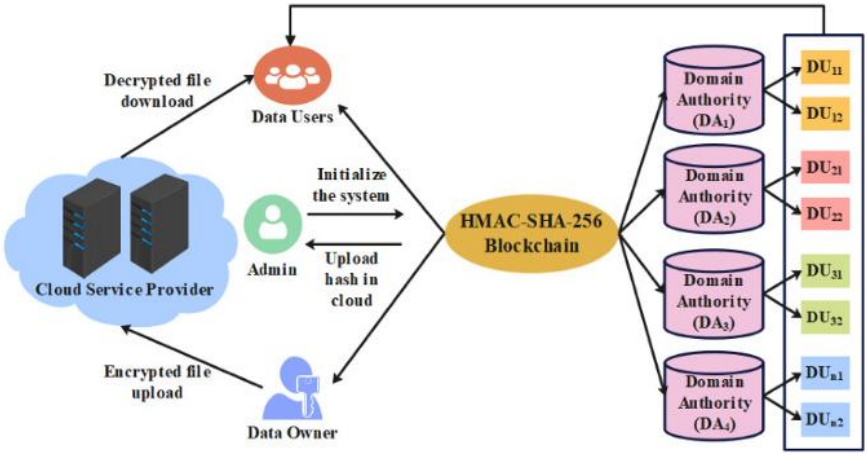

Figure 1. Semi-decentralized system utilizing HMAC with SHA-256

The one domain user has access to and saves data copies while other domain users are unable to access and transfer the data. When the data user needs to access data and upload it by the owner, the user accesses it from domain authority and decrypts actual content on their local machine through decryption. Here, dual level key management technique has developed; first the encryption time on the information holder and second Blockchain framework via forming hash value. HMAC serves as a cryptographic mechanism for authentication system in which a cryptographic hashing algorithm is applied concurrently with a symmetric key to determine both the authenticity and integrity of the message. HMAC is consists of a particular data block and a symmetric key with a secure hash code. SHA-256 is a hash algorithm that creates a constant-length 256 bits hash code algorithm. The Blockchain mechanism utilising hash message authentication code (HMAC) which implements secure hash algorithm techniques (SHA-256-bit), it is a very confidential and brief approaches to allocate or convey data. Message authentication is a procedure to verify the message authenticity in which two significant factors are taken into message authentication verification like source and the message are unable to be modified. Figure 2 presents the data-block structure for the whole message integrity verification procedure that contains a private key for producing information into the algorithm structure.

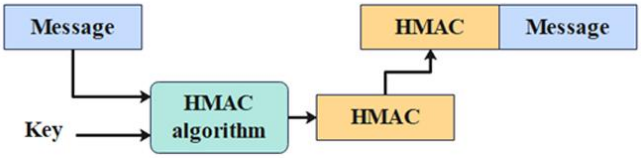

Figure 2. HMAC based message authentication process

The sender transmits the message with its MAC. At the receiver end, the received MAC is verified using the same secret key. If both MACs are similar, it confirms that no modifications have occurred to the message and it is sent by an authentic sender. The encryption-based HMAC is based on fixed-length-SHA-256bit was developed in this research to produce and validate signatures of multiple transactions, ensuring that the data is not tampered with or disclosed. The given input key is initially hashed any input text through HMAC and the input key is produced through XORing operation the Inner pad (Ipad) with input text(IP). The Ipad score is 36hex with 64byte timeout which is based on key length. The SHA-256 output of hash function is provided into next SHA-256 for generating HMAC output design. The key input is XORed by Outer pad (Opad) that has 5C scores in hex prior hashing primary SHA-256 output. The integration of 64byte key, K_0, Opad output and primary SHA-256 output are hashed together to generate HMAC output. The MAC is estimated by HMAC function over textual data presentation as shown in the equation. (1), Where, $\oplus$ and $||$ are denotes XOR and concatenation.

$$MAC(Messageinput)_t = HMAC(K, Messageinput)_t$$
$$H((K_0 \oplus Opad)||H((K_0 \oplus Opad)||Messageinput))_t \quad (1)$$

The score from Ipad is transferred to the primary SHA-256 design and the encrypted-based HMAC compute produces the result of the primary fixed-length-SHA-256bit to the next fixed-length-SHA-256bit to attain the whole HMAC produce output. Dual similar hash code method frameworks are utilized in HMAC architecture to attain its result, and it is used in HMAC architecture for the whole HMAC structure. As a output, of the primary fixed-length-SHA-256bit is implemented first, and the secondary SHA-256bit waits until it receives the message inputs from the outputs of the primary SHA-256bit implementation. Hence, the primary SHA-256 validity stays critical for obtaining resulting HMAC based SHA-256bit. The 64-bit states in the framework have a produced inputs sequences for primary and next SHA-256bit algorithms techniques. Totally 32-bit state are implemented of which 16 are for the primary 512 bits and the other 16 are for the next 512 bits to process the primary SHA-256 messages. The message uses the primary 512bit hash function result to attain the next 512bit result in the input message. The Ipad has a similar concept of inputting messages to the next SHA-256 and key Opad is integrated through the primary SHA-256 result. Like earlier SHA-256bit procedures, the result of the next 512-bit blocks in fixed-length-SHA-256bit process uses the result of the primary 512bit blocks from the another hash code functions.denotes the HMAC design structure with a dual SHA-256 hashing algorithm which presents how the Ipad data is incorporated by text input. Figure 3 shows the structure of HMAC-SHA-256.

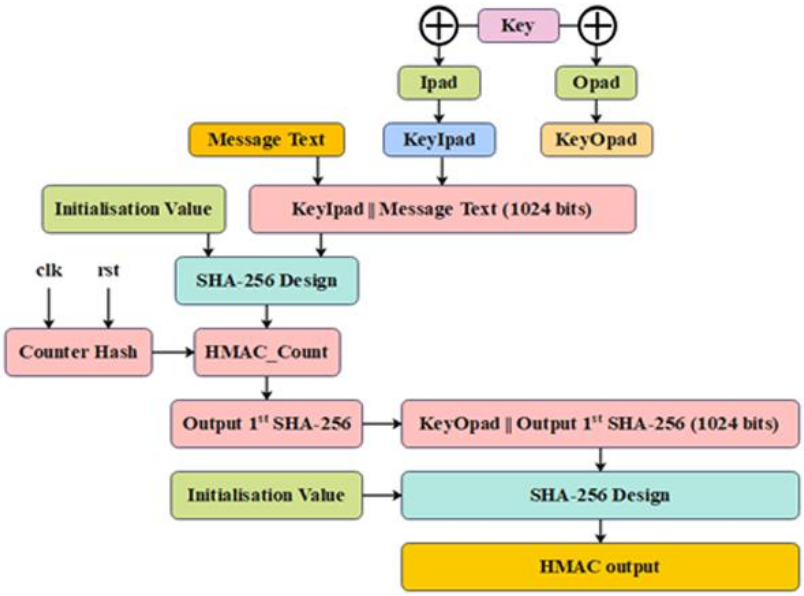

Figure 3. Structure of HMAC-SHA-256-bit

Some of the hash functions have properties such as fixed-length output and computational feasibility for defining x like that Hash (x) generated hash value. Similar hash codes are impossible to find, and these characteristics are established weak hash functions. Moreover, no pair (x, y) is found for that Hash$(x) =$

hash value, computationally (y). SHA-256 processed 512bit message input and 160bit primary score to generate 160bit hash code result. The input message block is padded prevously in the SHA-256bit operation and once it is received the messages is completed by data appending a single one-bit. Next n zero bit is included, and the pattern is continued until the number of message bits is similar. The message input ability is 512bits and its scheduler calculates the message W_t of SHA-256. For $0 \leq t \leq 15$, the message is directly extracted from input message while for $16 \leq t \leq 63$, the message W_t estimated by the equation. (2),σ_0^{256} and $\sigma_1^{256}$are presented in the (3) and (4),

$$W_t = messageinput\ 0 \leq t \leq 15$$
$$W_t = \sigma_1^{256}(W_{t-2}) + W_{t-7} + \sigma_0^{256}(W_{t-15}) + W_{t-16}\ 16 \leq t \leq 63 \quad (2)$$

$$\sigma_0^{256}(x) = ROTR^7(x) + ROTR^{18}(x) + SHR^3(x)(3) \quad (3)$$

$$\sigma_1^{256}(x) = ROTR^{17}(x) + ROTR^{19}(x) + SHR^{10}(x)(4) \quad (4)$$

Where, t is a number of transformation rounds,$ROTR^n(x)$ is a right rotation of x through n bits, $SHR^n(x)$ is a right shift of x through n bits. At last, the proposed HMAC-SHA-256 provides an output which secure and optimized data distribution in the Blockchain networks. The blockchain uses secure HMAC with SHA-256, it is a encrypted and streamlined method to broadcast or exchange data. The Algorithm 1 for secure HMAC-SHA-256-bit is given below.

Algorithm 1. HMAC-SHA-256-bit

Input : HMAC $(Key\ K, Msg\ M)$
Output : HMAC-SHA-256 code
Step 1 : if $(Len(K) > block\_size)$ then
$K = SHA - 256\,(K)$
Step 2 : if $(Len(K) < block\_size)$ then
Pad K with zeros to $block\_size$
Step 3 : $Inner\_pad = K \oplus ipad$
Step 4 : $Outer\_pad = K \oplus opad$
Step 5 : $Hash\_Inner = SHA - 256(Inner\_pad||M)$
Step 6 : $HMAC = SHA - 256(Outer\_pad||Hash\_Inner)$
Step 7 : Return HMAC

3. OUTCOMES AND DISCUSSION

The cryptographic hash code produced by the hash function of the SHA-256-bit is simulated in an environment of python language program code with computer system setup the Windows 11 Operating system, RAM 12GB, and Intel i9 processor. The several parameters such as The evaluation, considers retrieval time together with encryption and decryption speed and system throughput. for estimating the HMAC-SHA-256 efficiency. The different file sizes such as 50KB, 100KB, 150KB, 200KB, 250KB, and 300KB, are considered to analyze the retrieval time of HMAC-SHA-256. The different shared data sizes, such as 10MB-60MB, are considered to analyze the throughput of HMAC-SHA-256. The different shared data sizes, such as 1MB, and 10MB-40MB, are considered to analyze the encryption and decryption time of HMAC-SHA-256.

In Figure 4, the HMAC-SHA-256 performance is estimated by retrieval time with file sizes of 50KB, 100KB, 150KB, 200KB, 250KB, and 300 KB. The IPFS, Elliptic Curve Digital Signature Algorithm (ECDSA), HMAC, and SHA-256 are taken as state-of-art methods, and their performance is compared with HMAC-SHA-256. The HMAC-SHA-256 achieves best retrieval time of 0.4s, 1.0s, 1.5s, 1.9s, 2.2s, and 2.8s for the file size of 50KB, 100KB, 150KB, 200KB, 250KB, and 300KB, respectively. In Figure 5, the HMAC-SHA-256 performance is estimated by throughput with a shared data size of 10MB-60MB. The IPFS, ECDSA, HMAC, and SHA-256 is taken as state-of-the-art methods, and their performance is compared with HMAC-SHA-256. The HMAC-SHA-256 achieves the best throughput of 186, 185, 192, 187, 196, and 189 for the shared data size of 10MB-60MB, respectively.

In Figures 6 and 7, the performance of HMAC-SHA-256 is estimated based on encryption and decryption time for shared data sizes of 1MB, 10MB-40MB. The IPFS, ECDSA, HMAC, SHA-256 is taken as state-of-art methods and their performance is compared with HMAC-SHA-256. The cryptographic HMAC-SHA-256bit achieves the best encryption time of 6ms, 72ms, 122ms, 173ms and 245ms for the shared data size of 1MB, and 10MB-40MB correspondingly. Similarly, the hash code produced by the hash function of the SHA-256 bit achieves the leading decryption times of 3ms, 36ms, 47ms, 88ms and 123ms for the shared data size of 1MB, and 10MB-40MB correspondingly.

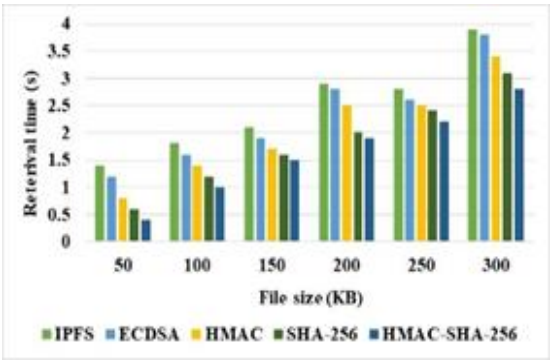

Figure 4. Retrieval time of HMAC-SHA-256

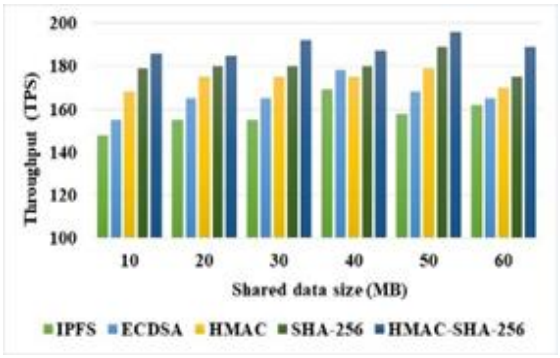

Figure 5. Throughput of HMAC-SHA-256

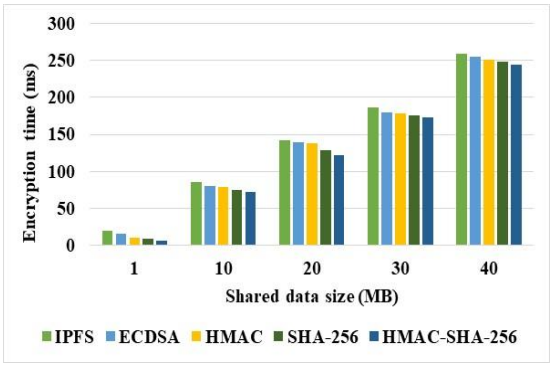

Figure 6. Encryption time of HMAC-SHA-256

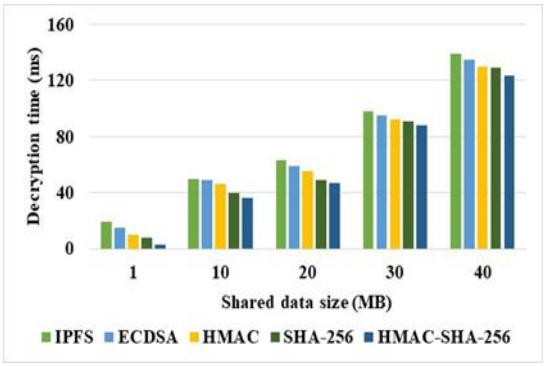

Figure 7. Decryption time of HMAC-SHA-256

3.1. Comparison study

The comparison study of Encryption-based HMAC-SHA-256-bit with existing techniques is discussed in this subsection in terms of retrieval time, together with encryption and decryption speed, and system throughput.. The existing methods, like IPFS [21] and IPFS-ECC file system [22], are taken and differentiated with HMAC-SHA-256. From Figure 8, the encryption-based HMAC-SHA-256-bit achieves the best retrieval times of 0.4s, 1.0s, 1.5s, 1.9s, 2.2s, and 2.8s for the file sizes of 50KB, 100KB, 150KB, 200KB, 250KB, and 300KB, correspondingly. From Figure 9, the HMAC-SHA-256 achieves the best throughput of 186, 185, 192, 187, 196, and 189 for the shared data size of 10MB-60MB, respectively. From Figure 10, the HMAC-SHA-256-bit achieves the most efficient decryption time of 3ms, 36ms, 47ms, 88ms, and 123ms for the shared data size of 1MB, 10MB-40MB correspondingly. From Figure 11, the encryption-based HMAC-SHA-256-bit achieves the most efficient decryption time of 3ms, 36ms, 47ms, 88ms, and 123ms for the shared data size of 1MB, 10MB-40MB correspondingly.

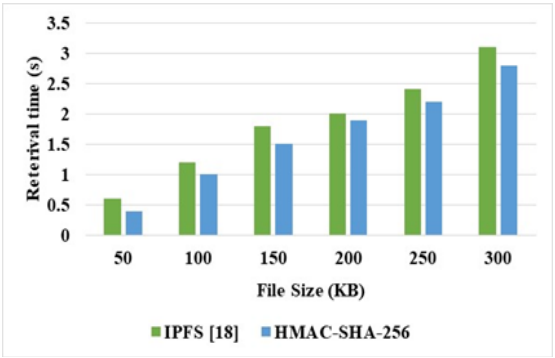

Figure 8. Comparison in terms of retrieval time

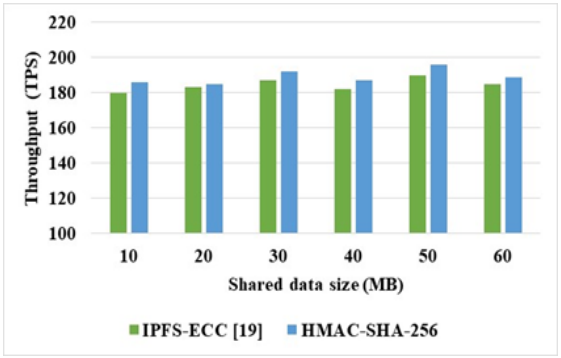

Figure 9. Comparison in terms of throughput

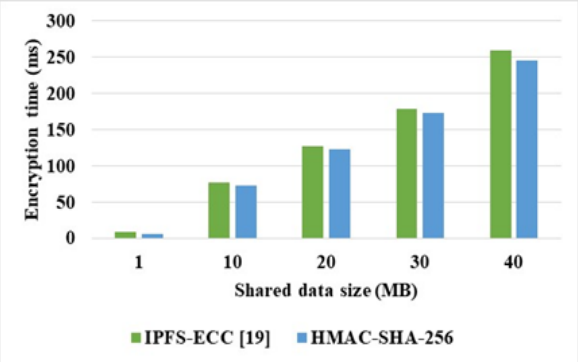

Figure 10. Comparison of encryption time

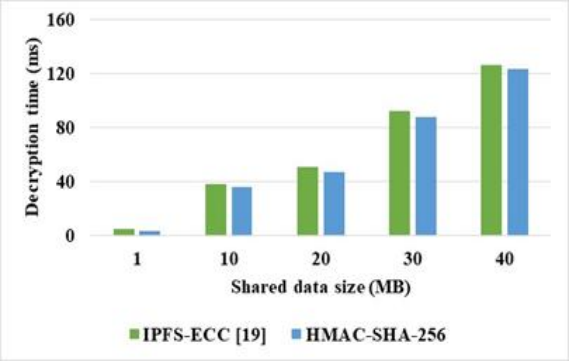

Figure 11. Comparison of decryption time

3.2. Discussion

The existing techniques such as IPFS [21] suffered from scalability and indeterminate key management for access control policies due to the utilization of searchable encryption algorithms. The IPFS-ECC [22] suffered from scalability and indeterminate key management for access control policies due to the utilization of searchable encryption algorithms. To overcome these problems, the encryption-based HMAC-SHA-256bit is proposed for encypted and effective information distribution in blockchain. The encryption-based HMAC is a secure cryptographic validation system in that a cryptographic secure hash function is employed with a symmetric key to establish both the source validation and data reliability of the message. In blockchain, the HMAC is implemented with fixed length SHA-256bit to generate and authenticate the signatures of several transactions. SHA-256 is a hash algorithm that creates a fixed-length-256-bit cryptographic hash. The blockchain utilizes encryption based HMAC is using SHA-256bit, it is a encrypted and concise approach to distribute or communicate data.

The result of this research shows that the HMAC-SHA-256 improves security for data sharing in blockchain through minimizing retrieval time, enhancing throughput and optimizing encryption and decryption process. The findings denote that the incorporation of HMAC with SHA-256 provides better cryptographic approach which measures data authentication and integrity thereby making it better for decentralized data sharing system. The obtained retrieval time and throughput enhances the method effectiveness specifically in large-scale data transmission.

4. CONCLUSION

In this manuscript, the encryption-based HMAC-SHA-256bit is proposed for encrypted and effective information exchanging in blockchain network. The encryption-based HMAC is a cryptographic access validation system in that cryptographic hashing function is utilized simultaneously with a private key to specify both the authenticity and integrity of the data block. HMAC is contains of a message and a encrypted key with a hash code. In Blockchain network, the encryption-based HMAC is utilized with fixed-length-SHA-256bit to generate and verify signatures of several transactions.SHA-256bit is a hash algorithm that creates a fixed-length-256-bit hash code. The blockchain uses encryption-based HMAC using SHA-256bit, it is a secure and concise approachs to distribute or communicate data. In this work, the file size of retrieval time is considered as 50KB, 100KB, 150KB, 200KB, 250KB and 300 KB. The shared data size of throughput is 10-60, encryption and decryption time is 1MB, 10MB-40MB. The HMAC-SHA-256bit achieves most effective message encryption time of 72ms and decryption time of 36ms for the shared data size of 10MB.The existing approaches suffer from indeterminate key management and scalability, HMAC-SHA-256 provides effective and secure data sharing through incorporating cryptographic hash functions with secret key. The key findings show that the model reduces the retrieval time, improves throughput, encryption and decryption time. The research sets new possibilities for future advancements that involve developing stronger cryptographic approaches alongside efficiency modifications and multiple blockchain system and decentralized cloud storage application. Future research aims to improve security measures of the system while adapting the method to new blockchain developments for sustainability and reliable performance.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Naveenkumar Lingaraju	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Manjula Haladappa Sunkadakatte		✓			✓	✓	✓			✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing -**O**riginal Draft
E : Writing - Review &**E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] S. Uppal, B. Kansekar, S. Mini, and D. Tosh, "HealthDote: a blockchain-based model for continuous health monitoring using interplanetary file system," *Healthcare Analytics*, vol. 3, p. 100175, Nov. 2023, doi: 10.1016/j.health.2023.100175.

[2] G. Xu, J. Zhang, U. G. O. Cliff, and C. Ma, "An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption," *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 10715–10750, Dec. 2022, doi: 10.1002/int.22946.

[3] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, and Y. Zhang, "A secure and privacy-preserving medical data sharing via consortium blockchain," *Security and Communication Networks*, vol. 2022, pp. 1–15, May 2022, doi: 10.1155/2022/2759787.

[4] Q. Zhang and Z. Zhao, "Distributed storage scheme for encryption speech data based on blockchain and IPFS," *Journal of Supercomputing*, vol. 79, no. 1, pp. 897–923, Jan. 2023, doi: 10.1007/s11227-022-04702-1.

[5] A. G. Alzahrani, A. Alhomoud, and G. Wills, "A framework of the critical factors for healthcare providers to share data securely using blockchain," *IEEE Access*, vol. 10, pp. 41064–41077, 2022, doi: 10.1109/ACCESS.2022.3162218.

[6] I. Khan and M. Haladappa, "Risk-Aware Multi-Agent Advantage Actor-Critic Based Resource Allocation for C-V2X Communication in Cellular Networks," *Proceedings of Engineering and Technology Innovation (PETI)*, vol. 29, pp. 47–60, Feb. 2025, doi:10.46604/peti.2024.14136.

[7] L. Hong, K. Zhang, J. Gong, and H. Qian, "A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing," *Security and Communication Networks*, vol. 2022, pp. 1–14, Sep. 2022, doi: 10.1155/2022/4978802.

[8] D. Brabin, C. Ananth, and S. Bojjagani, "Blockchain based security framework for sharing digital images using reversible data hiding and encryption," *Multimedia Tools and Applications*, vol. 81, no. 17, pp. 24721–24738, Jul. 2022, doi: 10.1007/s11042-022-12617-5.

[9] S. J. Hsiao and W. T. Sung, "Blockchain-Based Supply Chain Information Sharing Mechanism," *IEEE Access*, vol. 10, pp. 78875–78886, 2022, doi: 10.1109/ACCESS.2022.3194157.

[10] M. Bin Saif, S. Migliorini, and F. Spoto, "Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain," *Future Internet*, vol. 16, no. 3, p. 98, Mar. 2024, doi: 10.3390/fi16030098.

[11] C. Lai, Z. Ma, R. Guo, and D. Zheng, "Secure medical data sharing scheme based on traceable ring signature and blockchain," *Peer-to-Peer Networking and Applications*, vol. 15, no. 3, pp. 1562–1576, May 2022, doi: 10.1007/s12083-022-01303-w.

[12] G. Lin, H. Wang, J. Wan, L. Zhang, and J. Huang, "A blockchain-based fine-grained data sharing scheme for e-healthcare system," *Journal of Systems Architecture*, vol. 132, p. 102731, Nov. 2022, doi: 10.1016/j.sysarc.2022.102731.

[13] A. Liu *et al.*, "DynaShard: Secure and Adaptive Blockchain Sharding Protocol With Hybrid Consensus and Dynamic Shard Management," in *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 5462-5475, 1 March 1, 2025, doi: 10.1109/JIOT.2024.3490036.

[14] S. Sathiya Devi and A. Bhuvaneswari, "Design of efficient storage and retrieval of medical records in blockchain based on InterPlanetary File System and modified bloom tree," *Security and Privacy*, vol. 6, no. 5, Sep. 2023, doi: 10.1002/spy2.301.

[15] S. A. H. Mohsan, A. Razzaq, S. A. K. Ghayyur, H. K. Alkahtani, N. Al-Kahtani, and S. M. Mostafa, "Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system," *International Journal of Environmental Research and Public Health*, vol. 19, no. 22, p. 14641, Nov. 2022, doi: 10.3390/ijerph192214641.

[16] B. Li and M. Ma, "An advanced hierarchical identity-based security mechanism by blockchain in named data networking," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 13, Jan. 2023, doi: 10.1007/s10922-022-09689-x.

[17] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5045–5058, Sep. 2022, doi: 10.1016/j.jksuci.2021.05.002.

[18] R. Bhan, R. Pamula, P. Faruki, and J. Gajrani, "Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network," *Journal of Supercomputing*, vol. 79, no. 14, pp. 16233–16274, Sep. 2023, doi: 10.1007/s11227-023-05272-6.
[19] S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," *Internet of Things*, vol. 24, p. 100969, Dec. 2023, doi: 10.1016/j.iot.2023.100969.
[20] A. I. Basuki, D. Rosiyadi, H. Susanto, I. Setiawan, and T. I. Salim, "Privacy-preserving reservation model for public facilities based on public Blockchain," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 4, pp. 4418–4429, Aug. 2024, doi: 10.11591/ijece.v14i4.pp4418-4429.
[21] I. Khan and M. Haladappa, "Dynamic Resource Reservation using Deep Reinforcement Learning: Optimizing Resource Allocation for Platoon-Based C-V2X Networks," *Engineering Letters (EL)*, vol. 33, no. 5, pp. 1372–1381, May 2025.
[22] I. L. H. Alsammak, M. F. Alomari, I. Shakir Nasir, and W. H. Itwee, "A model for blockchain-based privacy-preserving for big data users on the internet of thing," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 26, no. 2, p. 974, May 2022, doi: 10.11591/ijeecs.v26.i2.pp974-988.
[23] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 152–167, Jun. 2022, doi: 10.1016/j.jpdc.2022.03.009.
[24] Z. Wang and S. Guan, "A blockchain-based traceable and secure data-sharing scheme," *PeerJ Computer Science*, vol. 9, p. e1337, Apr. 2023, doi: 10.7717/PEERJ-CS.1337.
[25] C. Liu, F. Xiang, and Z. Sun, "Multiauthority attribute-based access control for supply chain information sharing in blockchain," *Security and Communication Networks*, vol. 2022, pp. 1–18, Apr. 2022, doi: 10.1155/2022/8497628.
[26] J. L. Gao *et al.*, "Toward Efficient Blockchain for the Internet of Vehicles with Hierarchical Blockchain Resource Scheduling," *Electronics*, vol. 11, no. 5, p. 832, Mar. 2022, doi: 10.3390/electronics11050832.
[27] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, C. Verma, and Z. Illes, "Enhancing logistics with the internet of things: a secured and efficient distribution and storage model utilizing blockchain innovations and interplanetary file system," *IEEE Access*, vol. 12, pp. 4139–4152, 2024, doi: 10.1109/ACCESS.2023.3339754.

BIOGRAPHIES OF AUTHORS

Naveenkumar Lingaraju is a Research Scholar at the Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India. He completed his Bachelor's Degree in Computer Science and Engineering from Visvesvaraya Technological University and pursued a Master's in Computer Science and Engineering at UVCE, Bangalore. Naveenkumar L's expertise spans diverse domains, including cybersecurity, blockchain, computer networks, cloud security, data mining, firewalls and VPNs, cryptography, artificial intelligence, and machine learning in cybersecurity, cyber-physical system security, neural networks, edge computing, and cybersecurity in 6G networks. His commitment to pioneering research is demonstrated by his presentation of an IEEE conference paper, highlighting his enthusiasm for advancing technological knowledge and shaping the future of computer science and Network security systems. He can be contacted at email: naveengowdakns@gmail.com.

Manjula Haladappa Sunkadakatte currently a Professor in the Department of Computer Science and Engineering at the University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, has established herself as a prominent figure in the field. Holding a B.E., M.Tech., and Ph.D. in Computer Science and Engineering, she has honed her expertise in computer networks, wireless sensor networks, data mining, cloud computing, artificial intelligence, machine learning, and federated learning. Driven by a passion for knowledge, she has made significant contributions to these domains, evident through her scholarly publications and conference presentations. As an educator, her influence extends beyond the classroom, shaping the minds of future engineers. Dr. Manjula's holistic approach to academia, balancing research and teaching, underscores her commitment to advancing the frontiers of Computer Science and Engineering, leaving an indelible mark on both her students and the technological landscape at large. With an impressive track record, she has authored 69 journals, presented 72 conference papers, holds 5 patents, and has contributed to 4 book chapters while publishing 4 books, showcasing her prolific and diverse contributions to the academic and technological community. Additionally, Dr. Manjula is currently a respected member of the Executive Council and has served as a former member of the Academic Senate at VTU Belagavi. She can be contacted at email: shmanjula@gmail.com.