International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 26-33, January-2026
https://doi.org/10.47001/IRJIET/2026.101004

A Secure Blockchain-Based Communication System with Multimedia Encryption and Real-Time Consensus Visualization

[1]Jaafar S. Ali, [2]*Ayman N. Muhi, [3]Mustafa Ghanim, [4]Mohaimen Q. Algburi

[1,2,3,4]College of Communication Engineering, University of Technology- Iraq
*Corresponding Author's E-mail: aymen.n.muhi@uotechnology.edu.iq

***Abstract* - Safe communication is of essence in this digital age, particularly with the explosive increase in multimedia information. In this paper, the design and implementation of Secure Blockchain-Based Communication System that uses Fernet encryption on multimedia data (text, images, audio, and video) and blockchain technology to perform decentralized logging and real-time verification is presented. The suggested system will combine symmetric encryption and a tailor-made blockchain platform to provide confidentiality, integrity, and authenticity of the data transmitted. Every message is then encrypted with the help of a specific symmetric key and is stored on a blockchain, where Proof-of-Work (PoW) consensus ensures the data integrity. The graphical user interface (GUI) created with Python and Tkinter enables a user to communicate with the encryption and decryption modules, track real-time blockchain growth and performance indicators. The performance of the system was tested widely to prove that the system secured the multimedia data transmission and also could scale with the growth of the blockchain. The combination of blockchain delivers the impossibility of tampering with data validation, and the visualization of the real-time consensus gives a transparent insight into the inner workings of the blockchain, and the system is applicable in secure messaging with journalists, imaging in the medical field, and surveillance data.**

Keywords: Blockchain Technology, Multimedia Encryption, Fernet Encryption, Proof-of-Work (PoW), Python.

I. INTRODUCTION

In the contemporary era of ubiquitous digital communication, the secure transmission and storage of information have become paramount. The exponential growth of multimedia data—comprising text, images, audio, and video—across diverse platforms such as instant messaging applications, telemedicine services, smart surveillance systems, and video conferencing technologies, has intensified the demand for robust and adaptable encryption frameworks [1]. Ensuring the confidentiality, integrity, and authenticity of such information is now a foundational requirement in safeguarding against an increasingly complex array of cyber threats and data breaches [2].

However, multimedia encryption poses different and complex issues that are not similar to those that are related to conventional textual information. Video and audio streams are particularly high-bandwidth and latency-sensitive media files, in which selective or partial encryption may be applied to achieve a balance between performance and security. Also, the vulnerability of multimedia information to threats like unauthorized access, forgery, manipulation of content, and unauthorized redistribution needs context-sensitive and media-specific encryption measures. This means that the creation of secure multimedia communication systems should be able to take into consideration the heterogeneity and real-time features inherent in these formats [3-5]. Blockchain technology has become a revolutionary instrument in the past years to create decentralized trust and unattainable data verification in many fields. Blockchain, with its distributed consensus algorithm and tamper-evident ledger, has an attractive set of benefits to improving data integrity and accountability. However, its straightforward combination with multimedia encryption is rather under-researched. The storage and real-time processing of large media files are not natural characteristics of the traditional blockchain architecture. Nevertheless, in combination with an external encryption layer, blockchain can be used as a secure level of logging and verification, making it a central point of establishing traceable and tamper-proof communication environments [6-7]. This paper introduces the design and implementation of a Secure Blockchain-Based Communication System Multimedia Encryption and Real-Time Consensus Visualization. The suggested system is a synergistic combination of symmetric encryption methods, namely the Fernet encryption standard, and a bespoke blockchain framework. It facilitates safe reception and confirmation of four different data types: text information, pictures, audio messages, and video files. Both confidentiality and traceability are provided by each modality being encrypted individually and then linked to a cryptographically verified blockchain transaction [8-9].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 1, pp 26-33, January-2026

https://doi.org/10.47001/IRJIET/2026.101004

Symmetric keys are used to encrypt text messages, and they are hashed before being registered on blockchain. The data of the images are encrypted, processed, and stored with integrity tags stored on-chain. Audio data are encrypted using format specific algorithms and are checked prior to play, and video files are encrypted frame by frame and metadata are hashed to maintain fidelity and authenticity of the content. These activities are coordinated with a single graphical user interface (GUI) created with Python and Tkinter, which allows non-expert users to interact with the modules of encryption, decryption, and blockchain verification without any difficulties [10-11]. Practical reasons to come up with such a system are based on various practical applications. These are: secure communications to journalists and whistleblowers in hostile areas, secure delivery and storage of medical imaging in the healthcare systems, secure transmission of surveillance video streams in smart cities, and the storage of sensitive voice and video content in distributed ledgers to aid in forensic or legal processes. Through these needs, the proposed system has shown a scalable and modular solution, which can be functional across various domains and application levels [12-13]. One of the characteristics of the system is that it can visually show real-time consensus, which is otherwise not possible with many implementations of blockchain. This visualization layer provides information on what goes on in the blockchain, such as the process of mining of blocks, iteration of nonce, and validation of hash. This property does not only facilitate the transparency of the system, but it is also a priceless educational, debugging and auditing tool, increasing user confidence and knowledge.

One of the most developed fields of information security is the encryption of texts, where AES, RSA, and ECC are the most commonly used methods of ensuring the safety of communication. Homomorphic encryption lets you compute on encrypted data, such that cloud-based messaging can be done securely without revealing plaintext. Gao et al. [14] introduced a chat that uses homomorphic encryption which improves privacy of messaging apps. However, such systems remain centralized and vulnerable to server-side threats. In image encryption, machine learning-based segmentation models have shown promise. Wu et al. [15] proposed the Medical SAM Adapter, integrating domain-specific medical knowledge for privacy-preserving segmentation. While effective in healthcare, these methods lack blockchain integration and general-purpose applicability. Similarly, Roy et al. [16] explored prompt-based zero-shot segmentation but did not address data security or decentralization. Audio encryption has traditionally emphasized physical-layer transmission in complex media. Flatté [17] examined underwater acoustic signal variability, using path integrals to predict wave behavior. While conceptually valuable, such work is not designed for real-time user communication. More recent systems aim for practical encryption solutions but rarely leverage blockchain for tamper-proof verification. Video encryption, particularly for large-scale or streaming data, poses major challenges. Tang et al. [18] surveyed the role of large language models (LLMs) in video understanding, categorizing approaches such as Video Analyzer × LLM. However, security and blockchain integration were largely absent. Maaz et al. [19] proposed Video-ChatGPT for rich video-text interaction, yet it depends on centralized AI APIs and does not support encryption or verifiable transaction records.

Some studies have investigated blockchain-enabled multimedia frameworks. Ma et al. [20] proposed a blockchain-based digital rights management (DRM) solution using smart contracts, focusing on ownership verification rather than communication. Similarly, Aujla et al. [21] explored blockchain for IoT data integrity, but not multimedia encryption or user-facing applications. Meanwhile, there was an emphasis on making the communication systems more secure and efficient by applying blockchain technologies, multimedia encryption, and displaying the real-time consensus. The suggested system makes use of the most recent encryption methods to approach multimedia content, making a guarantee of the methodology of the messages, pictures, and video-tapes in the process of distribution across the popular networks that are unfixed. The system also uses the immutable ledger of blockchain to offer an open and tamper-free space to validate the messages and reach a consensus.

Symmetric encryption algorithms such as Fernet are applied whenever transmitting and receiving multimedia data within the system as each piece of data or message is encrypted and then placed into the blockchain. The blockchain does not only help to keep the data safe but it also helps to achieve the real-time consensus by accepting Proof of Work (PoW) by various nodes in the network to confirm that the encrypted message blocks are true. A graphical interface displays the growth of blockchain and its consensus in real-time, thus a user is able to visibly see how the chain extended with succeeding blocks. The solution aims at the increased demand of secure and efficient communications in different domains, such as finance, healthcare, and the general passing of information by uniting cryptographic approaches, blockchain security, and improved visualization methods. Finally, the piece shows the promise of bringing these technologies together in order to develop a mature and sustained communication network.

II. SYSTEM DESIGN AND ARCHITECTURE

The proposed secure communication framework is based on the system architecture that involves multimedia encryption

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 26-33, January-2026
https://doi.org/10.47001/IRJIET/2026.101004

and blockchain technology that secure the confidentiality, integrity, and authenticity of transmitted data. The architecture allows safe transfer of any type of data: text, image, audio, video by encrypting each type of media through specific protocols and storing the encrypted data on a decentralized blockchain. The system additionally has real-time visualization of the consensus, which allows users to track the expansion of the blockchain and the verification of consensus in a variety of nodes. Figure. 1 represents the flow of the secure communication system with a special focus on the process of data encryption to blockchain transmission and consensus realization. The process starts with the sender uploading a message in various formats (Text/Image/Audio/Video). The message is then converted into an encrypted form, which includes relevant metadata such as sender, receiver, and timestamp. The encrypted message is then added to the blockchain for secure transmission. On the receiver's side, the message is retrieved and decrypted from the blockchain. Throughout the process, real-time consensus is maintained via the blockchain network to ensure that all nodes remain synchronized. This architecture ensures secure, encrypted communication and integrity validation.

The encrypted message, along with its metadata, is then added as a new block in the blockchain, ensuring that the transmission is securely logged. The message undergoes consensus across multiple nodes to ensure its validity, utilizing a Proof of Work (PoW) mechanism to prevent tampering or fraud. The receiver retrieves the encrypted message from the blockchain, and using the same encryption key, decrypts the message to retrieve the original content. The system continuously monitors the real-time synchronization and consensus across nodes, ensuring that all participants have an identical, tamper-proof version of the blockchain.

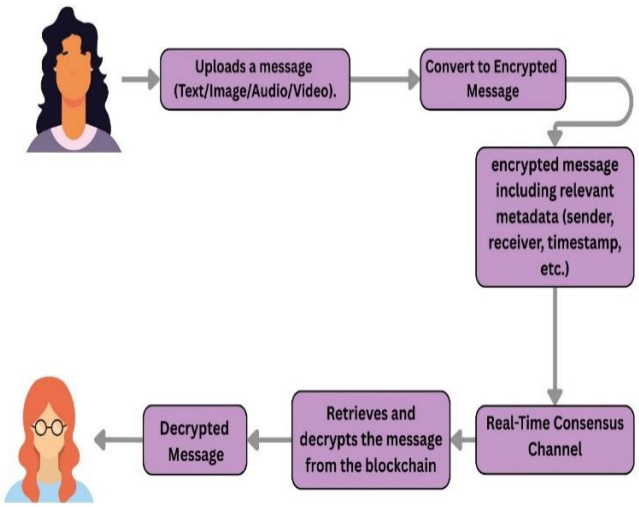


Figure 1: Workflow of Encrypted Multimedia Transmission Message

III. METHODOLOGY

The implementation methodology of the suggested secure communication system was organized according to the systematic approach to development that included the choice of encryption algorithms, blockchain design, multimedia management, and real-time visualization.

The system was developed to facilitate safe transfer of four data types namely; text, image, audio, and video. Different data types needed specific encryption and processing because they were available in different forms, sizes and processing requirements. Python and Tkinter were used to develop a GUI based desktop application to allow a non-technical user to interact with the product in an user-friendly manner.

In order to guarantee data confidentiality, Fernet symmetric encryption scheme (part of the cryptography library) was used because it is simple, strong and applicable to all media. A special symmetric key was created on the runtime and applied to encrypt and decrypt data in all operations. Text messages were encrypted using strings and the Imagery, audio and video files were read in binary streams and encrypted with the same Fernet key.

A custom blockchain written in Python was used to give tamper-evident logging and verifiability. The metadata that are included in each block are sender, receiver, timestamp, and the encrypted message. Block hashes were calculated with the help of the SHA-256 hash function.

PoW consensus was implemented by block hashes beginning with four leading zeros and the blockchain was simulated on three nodes to show distributed validation and consensus.

Individual modules to process various media types were used. The Encryption and decryption of images are carried out with Python Imaging Library (PIL) and displayed in the Graphical User Interface (GUI). Encryption of videos as binary, decryption and playback of videos using OpenCV, and the audio files are handled using PyDub as the audio files are decrypted and played back. Every module was able to make sure that media could be sent safely, decrypted and confirmed with the blockchain mechanism.

To illustrate the blockchain growth and promote the transparency, two kinds of plots were created. Blockchain Growth Plot that Plots block timestamps versus block indices with matplotlib and Performance Charts that Plot encryption/decryption timing and mining performance of various media types. Such visualizations assisted in the

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 26-33, January-2026
https://doi.org/10.47001/IRJIET/2026.101004

analysis of the time complexity, efficiency, and synchronization behavior of the system.

To formally outline the elements of the proposed secure communication system we introduce a mathematical model to describe the encryption process, blockchain structure, proof-of-work mechanism and consensus protocol.

3.1 Message Encryption

Let **M** represent the original plaintext message and **K** be the symmetric key generated using the Fernet algorithm. The encrypted ciphertext **C** is produced by the encryption function $E_K(\cdot)$, and decrypted by the inverse function $D_K(\cdot)$: Then,

$$C = E_{K(M)},\ and\ M = D_{K(C)} \qquad (1)$$

This encryption process is applied to all multimedia types—text **T**, image data **I**, audio **A**, and video **V**:

$$C_T = E_{K(T)}, \quad C_I = E_{K(I)}, \quad C_A = E_{K(A)} \quad and \quad C_V = E_{K(V)} \qquad (2)$$

3.2 Blockchain Block Structure

Each block B_i in the blockchain is defined as:

$$B_i = \left(i, H_{\{i-1\}}, t_i, C_i, S_i, R_i, N_i, H_i\right) \qquad (3)$$

Where:

- i: block index
- $H_{\{i-1\}}$: hash of the previous block
- t_i: timestamp
- C_i: encrypted content (text, image, audio, or video)
- S_i, R_i: sender and receiver identities
- N_i: nonce
- H_i: hash of the current block

3.3 Block Hash Calculation

The block hash H_i is computed using the SHA-256 hashing function:

$$H_i = SHA256\left(i \parallel H_{\{i-1\}} \parallel t_i \parallel C_i \parallel S_i \parallel R_i \parallel N_i\right) \quad (4)$$

Where ‖ denotes string concatenation.

3.4 Proof of Work (PoW)

To validate a block, a proof-of-work condition must be satisfied. The goal is to find a nonce N_i such that the resulting hash begins with a specific number of leading zeros:

$$\exists N_i \in N \quad such\ that \quad N_i[1:k] = 0 \qquad (5)$$

In this system, $k = 4$, requiring the hash to begin with four leading zeros. Where ∈ is an element of symbol and ∃ denotes to an existential quantifier.

3.5 Consensus across Nodes

Let $N = \{n_1, n_2, \ldots, n_N\}$ denote the set of participating nodes. Consensus is achieved if all nodes agree on the blockchain state:

$$\forall n_j \in N, \quad B_i \in C_j \quad \Rightarrow \bigcap_{j=1}^{N} C_j = C \qquad (6)$$

Where C_j is the chain view of node $\boldsymbol{j}$, and C is the agreed-upon blockchain. Also ∀ is a universal quantifier symbol, ∩ denotes to a set of intersection.

3.6 Real-Time Visualization

The real-time growth of the blockchain is modeled as a time-indexed mapping:

$$G(i) = (T_i, i)$$

Where T_i is the timestamp of the $i-th$ block, used for plotting blockchain expansion and observing dynamics of consensus.

Figure 2 illustrates the sequential process of secure message transmission using blockchain technology. The process begins with the sender uploading a message, which may be in the form of text, image, audio, or video. The uploaded message is then encrypted using Fernet encryption, a symmetric encryption method, followed by the generation of relevant metadata, including details such as the sender, receiver, and timestamp. Subsequently, the encrypted message, along with the associated metadata, is encapsulated into a new block within the blockchain.

The newly created block undergoes a Proof of Work (PoW) validation mechanism to ensure that the block meets the required computational criteria before it is considered valid. Upon successful validation, the block is broadcasted across the network to all participating nodes for consensus. Once consensus is achieved, the receiver retrieves the encrypted message from the blockchain, decrypts it using the appropriate key, and the decrypted content is displayed to the recipient. This process ensures secure, auditable, and decentralized message transmission.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 1, pp 26-33, January-2026

https://doi.org/10.47001/IRJIET/2026.101004

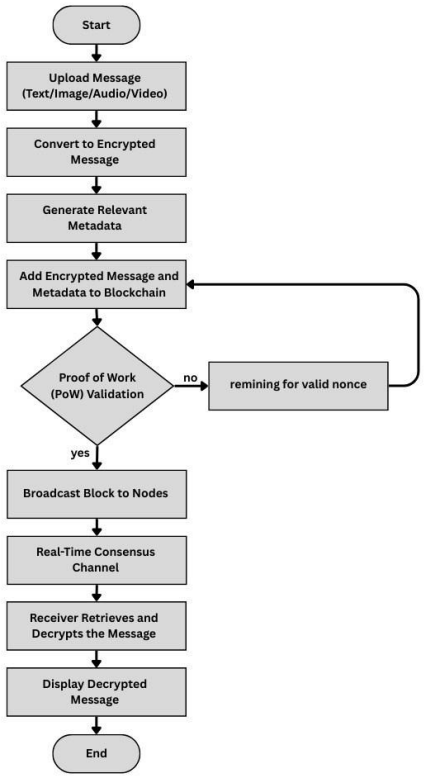


Figure 2: Program Flow chart

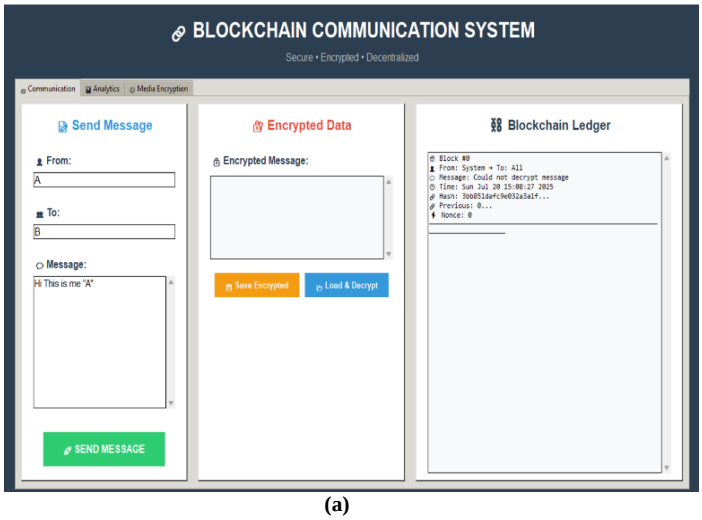
IV. IMPLEMENTATION AND RESULTS

4.1 System Implementation

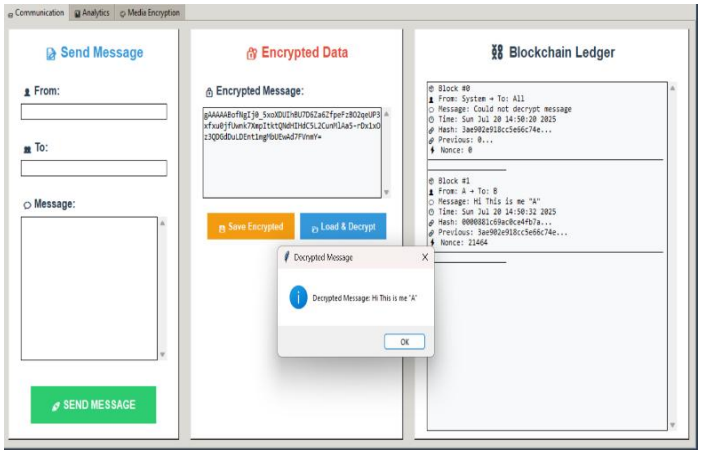
Secure Blockchain-Based Communication System was developed with Python programming language with libraries like Tkinter to create graphical user interface (GUI), cryptography to perform encryption, and hashlib to perform hashing of the block chain. The system was created to provide an opportunity to transfer and store multimedia data (text, images, audio, and video) in a secure way with the help of symmetric encryption (Fernet) and blockchain structure.

The GUI was developed in Tkinter and contains three major tabs, namely Communication, Analytics, and Media Encryption. The Communication Tab see Figure 3. gives the user the opportunity to enter the sender and receiver details, write a message and encrypt it to be stored on the blockchain. Analytics Tab Figure 4. provides real-time information on the development of the blockchain and performance rates. The Media Encryption Tab sees Figure 5 allows the user to encrypt as well as decrypt multimedia files, such as images, audio, and video with the same cryptographic framework.

Messages and multimedia data were encrypted with Fernet encryption in the backend to provide confidentiality and integrity. The symmetric key that was used to encrypt each message was different and the messages were then stored in the block chain. In the chain, all the blocks contain metadata, including the sender, the receiver, the timestamp, and the hash of the previous block, and the Proof-of-Work (PoW) algorithm makes sure that only the solution to a problem can make the block valid.



(a)



(b)

Figure 3: Encrypted Message Communication and Blockchain Ledger (a): Before Decryption; (b): After Decryption

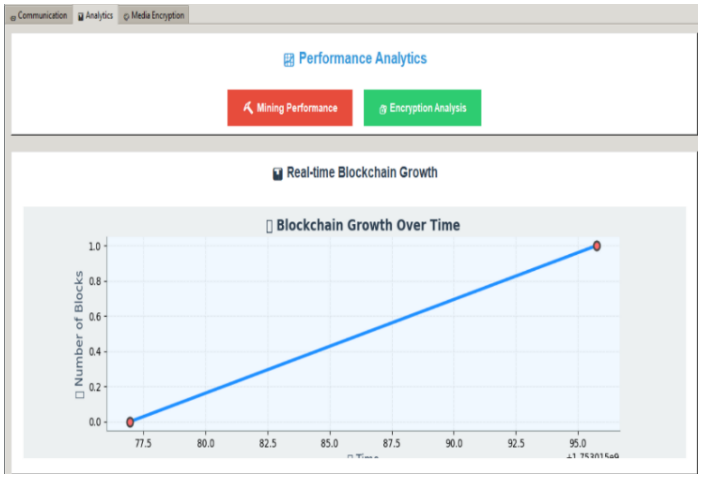


Figure 4: Analytics Tab - Real-Time Blockchain Growth and Performance Metrics

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 1, pp 26-33, January-2026

https://doi.org/10.47001/IRJIET/2026.101004

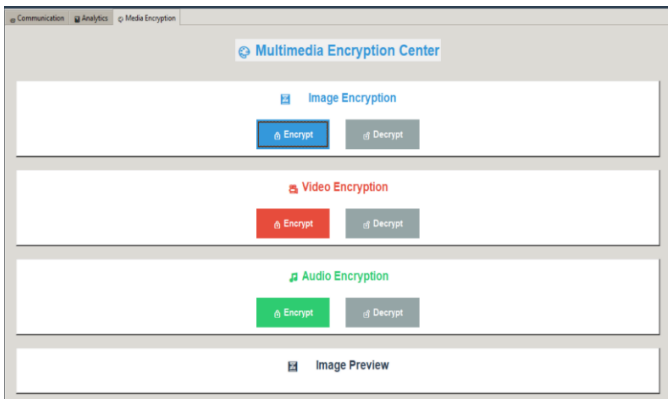


Figure 5: Media Encryption Tab - Encryption and Decryption of Multimedia Files

4.2 Results and Performance Evaluation

The system performance was measured by the number of successful message encryptions and decryptions, the expansion of the blockchain and the effectiveness of the consensus mechanism. During the testing, the system was able to encrypt and decrypt wide range of media (text, images, audio, video). The log of the encrypted messages was safely stored in the blockchain and the user could read and decrypt it correctly using the same encryption key. The GUI Blockchain Ledger area see Figure 3. showed the metadata of each block, such as the sender, receiver, date and time, and the message which was encrypted. Blockchain expanded as new messages were sent in real-time, and the number of blocks expanded in the Blockchain Growth Plot see Figure 4, which graphically followed the chain expansion over time. This proved the scalability of the system since it could process several messages and expand the blockchain accordingly.

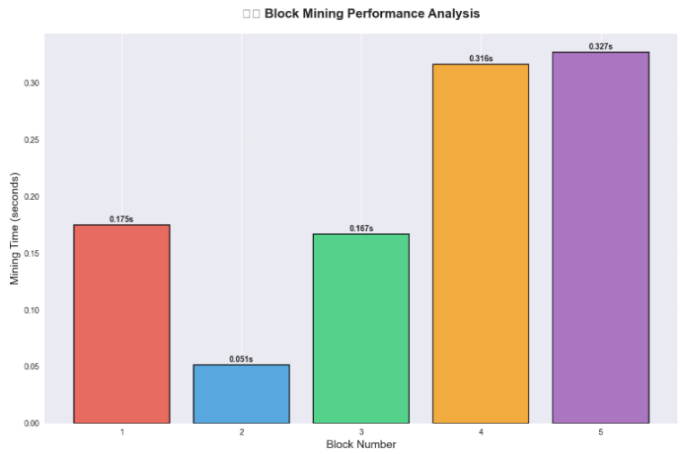


Figure 6: Mining Performance Analysis - Time Spent On Proof-Of-Work for Each Block

The performance of the mining of each block was assessed in terms of time spent during Proof-of-Work procedure. The findings, as shown in the Mining Performance Analysis bar graph see Figure 6 indicated that all the blocks were taking the same amount of time to mine except block number 4 and 5 that was taking more time because the computational difficulty in hitting the right nonce was higher. Such unpredictable mining time is normal when PoW is used to validate the blockchain.

Regarding the performance of encryption and decryption, the system could encrypt and decrypt the various data types, where text encryption was slower than image, audio or video because only text files were involved in the encryption during the test. This was depicted in the Encryption & Decryption Performance bar chart Figure 7 whereby the time of encryption of text was significantly longer.

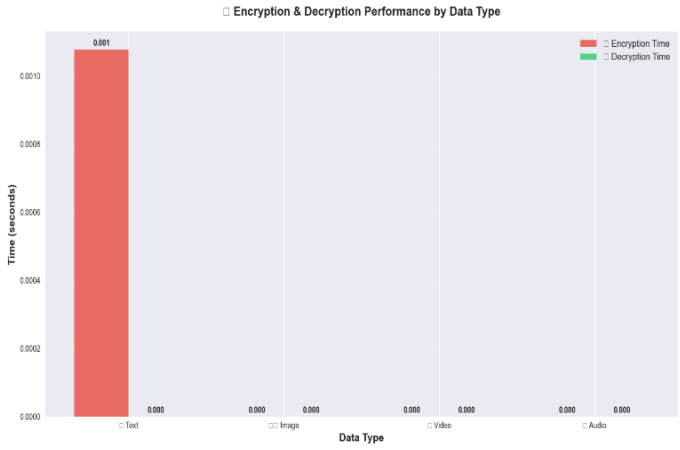


Figure 7: Encryption & Decryption Performance - Time Analysis for Various Data Types

V. CONCLUSION

This research suggested a new Secure Blockchain-Based Communication System, which is a combination of the latest encryption methods and blockchain technology to provide secure, immutable communication of multimedia data. The system is able to encrypt text, pictures, audio, and video files and store them in a decentralized blockchain ledger that cannot be tampered with and that is traceable. With the Proof-of-Work (PoW) mechanism, the consensus is reached among several nodes, and the data validity in the decentralized environment is guaranteed. Real-time visualization capabilities are also present in the system and monitor blockchain expansion and provide a view of the consensus process, which increases transparency and trust.

This system implementation is an indicator of its applicability in different fields, such as secure communication systems to whistleblowers, healthcare systems used in medical imaging, and smart cities as secure video surveillance. Nevertheless, the system can be still optimized in the aspect of performance, particularly with big multimedia files, and

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 26-33, January-2026
https://doi.org/10.47001/IRJIET/2026.101004

scalability by integrating more advanced blockchain frameworks e.g. Ethereum or Hyperledger. The future work will be aimed at enhancing the speed of the encryption/decryption process, expansion of the media types supported and user interface improvement to make the application more general. This system is an opportunity on the way to combining blockchain and encryption technologies to develop safe, efficient, and open communication solutions in the era of digitalization.

REFERENCES

[1] M. Ozaif, S. Mustajab, and M. Alam, "Exploration of Secured Data Transmission in the Internet of Things: A Survey," *Power and Communication*, 2024. [Online] Available: [HTML]

[2] O. Layode, H. N. N. Naiho, and G. S. Adeleke, "Data Privacy and Security Challenges in Environmental Research: Approaches to Safeguarding Sensitive Information," *Journal of Applied ...*, 2024. [Online] Available: ResearchGate.net

[3] K. M. Hosny, M. A. Zaki, N. A. Lashin, and M. M. Fouda, "Multimedia Security Using Encryption: A Survey," *IEEE*, 2023. [Online] *Available: IEEE.org*

[4] O. A. Khashan, N. M. Khafajah, W. Alomoush, and M. Alshinwan, "Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-core Processors," *Cryptography*, 2023. [Online] Available: MDPI.com

[5] S. Yin, H. Li, L. Teng, A. A. Laghari, and V. V. Estrela, "Attribute-Based Multiparty Searchable Encryption Model for Privacy Protection of Text Data," *Multimedia Tools and Applications*, vol. 2024, Springer. [Online] Available: ResearchGate.net

[6] F. Mlika, W. Karoui, and L. B. Romdhane, "Blockchain Solutions for Trustworthy Decentralization in Social Networks," *Computer Networks*, 2024. [Online] Available: [HTML]

[7] R. Lal, A. Chhabra, and S. Singla, "Blockchain Technology: Revolutionizing Trust, Transparency, and Transaction Efficiency," *International Conference on ..., 2024*. [Online] Available: [HTML]

[8] E. I. Zafir, A. Akter, M. N. Islam, S. A. Hasib, and T. Islam, "Enhancing Security of Internet of Robotic Things: A Review of Recent Trends, Practices, and Recommendations with Encryption and Blockchain Techniques," *Internet of Things, vol. 2024, Elsevier. [Online] Available: ScienceDirect.com*

[9] M. Y. Shakor, M. I. Khaleel, M. Safran, and S. Alfarhood, "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security," *IEEE, 2024. [Online] Available: IEEE.org*

[10] M. J. Mihaljević, M. Knežević, D. Urošević, L. Wang et al., "An Approach for Blockchain and Symmetric Keys Broadcast Encryption-Based Access Control in IoT," *Symmetry, 2023. [Online] Available: MDPI.com*

[11] M. A. Shawky, M. Usman, D. Flynn, and M. A. Imran, "Blockchain-Based Secret Key Extraction for Efficient and Secure Authentication in VANETs," *Journal of Information*, vol. XX, no. YY, pp. ZZ-ZZ, 2023. [Online] Available: ScienceDirect.com

[12] J. R. Henrichsen, "Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the 'Security Champion'," *Journalism and Safety*, 2024. [Online] Available: [HTML]

[13] K. Assmann, "Whistleblowers and Their Faith in Journalism," *Journalism Practice*, 2024. [Online] Available: [HTML]

[14] X. Gao, M. Huang, H. Luo, and Y. Xu, "A Homomorphic Encryption-Based Secure Chatting System," *IEEE Access*, vol. 8, pp. 132135–132144, 2020.

[15] J. Wu et al., "Medical SAM Adapter: Adapting Segment Anything Model for Medical Image Segmentation," *arXiv:*2304.12620, 2023.

A. Roy et al., "SAM Fails in Medical Images," arXiv:2304.05396, 2023.

[16] S. M. Flatté, "Sound Transmission Through a Fluctuating Ocean," *Stanford Research Institute, Tech. Rep*. JSR-76-39, 1977.

[17] Y. Tang et al., "Video Understanding with Large Language Models: A Survey," *arXiv:*2312.17432, 2024.

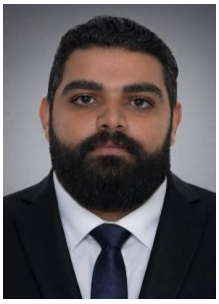
[18] M. Maaz et al., "Video-ChatGPT: Detailed Video Understanding via Large Vision and Language Models," *arXiv:*2306.05424, 2023.

[19] X. Ma, Y. Jiang, and C. Lin, "A Blockchain-Based Digital Rights Management System for Multimedia Content," *IEEE Trans. Multimedia*, vol. 24, pp. 142–153, 2022.

[20] G. S. Aujla et al., "Blockchain-Based Multimedia Content Protection: Challenges and Future Directions," *Multimedia Tools and Applications*, vol. 79, pp. 31533–31558, 2020.

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 26-33, January-2026
https://doi.org/10.47001/IRJIET/2026.101004

AUTHORS BIOGRAPHY



Jarfar Salim Ali is an Iraqi researcher. He earned his BSc degree in Electrical Engineering from the University of Technology, Baghdad, Iraq, in 2021. His academic and practical interests include programming and embedded systems, with experience in Arduino, Python, MATLAB, C#, and Raspberry Pi. His research interests focus on the integration of electrical engineering with software development for simulation, analysis, and implementation of engineering systems. He is particularly interested in automation, control systems, and smart technologies, and is actively working on developing his skills in these areas through continuous learning and applied projects.

Ayman N. Muhi is an Iraqi researcher. He earned his BSc and MSc degrees in Electronics and Communications Engineering from Al-Nahrain University, Baghdad, Iraq, in 2012 and 2016, respectively. During his MSc degree, he worked on a CubeSat communications design project. He has over 11 years of professional experience working with leading mobile communications equipment providers, such as Ericsson and Huawei. In 2023, he joined the University of Technology in Iraq as a lecturer. His research interests include the design and simulation of satellite communications systems, antenna design and modeling, fiber optic communications, 5G networks, and beyond. He also has extensive experience in the telecommunications sector, with proven expertise in microwave equipment, optical transmission, and their embedded systems.

Mustafa Ghanim received his B.Sc. degree in Computer Communication Engineering from Al-Rafidain University College, Baghdad, Iraq, in 2012. He obtained his M.Eng. degree in 2015 and his Ph.D. degree in Electrical Engineering in 2019 from Universiti Teknologi Malaysia (UTM), Johor, Malaysia. In 2021, he was a lecturer at the Department of Medical Instrumentation Engineering, Ashur University College. In 2023, he joined the College of Communication Engineering at the University of Technology- Iraq. His research interests include radio wave propagation, energy harvesting antennas, fifth-generation (5G) communications, satellite propagation, antennas and propagation, as well as the design and simulation of wireless communication systems, optical transmission, The IoT and AI applications are among his interests.

Mohaimen Q. Algburi is an Iraqi researcher specializing in advanced communication systems. He earned his B.Sc. degree in Systems Engineering from the University of Technology, Baghdad, Iraq, in 2013. In 2019, he was awarded a scholarship to pursue his Master's studies in Turkey, where he obtained a Master's degree in Electrical and Computer Engineering from Altınbaş University. Since 2023, he has been working as a lecturer at the University of Technology- Iraq. His research interests encompass the design and simulation of wireless power transfer, wearable antennas, body area networks, smart antennas, electromagnetic wave scattering by complex objects, 5G/6G technologies, and beyond. Fiber optic communications systems, the Internet of Things, and artificial intelligence are a part of his interests.

Citation of this Article:

Jaafar S. Ali, Ayman N. Muhi, Mustafa Ghanim, & Mohaimen Q. Algburi. (2026). A Secure Blockchain-Based Communication System with Multimedia Encryption and Real-Time Consensus Visualization. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(1), 26-33. Article DOI https://doi.org/10.47001/IRJIET/2026.101004

****

