NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

Developing A Lightweight Homomorphic Encryption Technique for Secure Data Transmission

Sumaira Bashir [1,*], **Amit Sharma** [2]

[1,2] School of Computer Applications, Lovely Professional University, Phagwara, Punjab, India

***** Corresponding Author: **Sumaira Bashir**, Email: Sumaira13579@gmail.com.

Abstract: This paper proposes a lightweight homomorphic encryption (HE) technique designed for secure data transmission in resource-constrained environments such as IoT, sensor networks, and edge computing platforms. The method integrates a modified AES structure—in which the number of rounds and key-expansion operations are optimized—with RSA's multiplicative homomorphism to support limited encrypted computation while minimizing computational overhead. The modified AES reduces complexity in the Mix Columns and Key Expansion stages without compromising cryptographic soundness. Experiments conducted on a 32-bit ARM-based emulator (100 MHz) and Arduino-class microcontroller demonstrate reduced encryption time, lower energy consumption, and improved throughput compared with standard AES, RSA, and AES+RSA hybrids. Preliminary comparisons with lightweight HE baselines (LWE-based and CKKS variants) indicate promising efficiency advantages for constrained hardware. Security analysis confirms that modifications do not weaken resistance against known cryptanalytic attacks. The resulting framework is suitable for healthcare monitoring, smart grids, industrial IoT, and privacy-preserving cloud analytics.

Access this article online

Keywords: Cloud–Edge computing security, Homomorphic encryption, Hybrid encryption schemes, IoT security, Lightweight encryption, Privacy-Preserving data processing

1. Introduction

SECURE data transmission is increasingly critical in the digital age, especially for resource-constrained devices in IoT and edge computing, which lack the capacity to handle traditional encryption efficiently. These methods also require decryption before processing, posing privacy risks. Homomorphic encryption (HE) addresses this by enabling operations on encrypted data, maintaining confidentiality even in untrusted environments. This allows lightweight devices to offload processing securely to more powerful servers. Cloud computing offers scalability and cost-efficiency but introduces data security risks due to its shared-resource model. Cryptographic solutions like RSA and elliptic curve cryptography (ECC) are used to secure communication and reduce key sizes for constrained devices. Attribute-Based Encryption (ABE) provides fine-grained access control, ideal for dynamic, sensitive environments such as healthcare. However, methods like AES and DES do not meet the performance and energy demands of modern IoT scenarios.

This paper proposes a lightweight homomorphic encryption approach that combines efficiency and strong data protection, making it suitable for IoT, healthcare, smart grids, and industrial environments.

Traditional encryption methods like AES and DES fall short in meeting the security and performance demands of

Received February 10, 2025; Revised March 11, 2025; Accepted April 10, 2025; Published June 31, 2025
https://doi.org/10.57238/csj.2025.1018

modern data transfer, highlighting the need for lightweight, efficient encryption techniques suitable for resource-constrained devices [1].

Homomorphic encryption enables secure computations on encrypted data without decryption, effectively reducing the risk of data breaches by allowing sensitive information to be processed and transmitted in encrypted form [2].

Traditional encryption methods such as AES and DES are inadequate for modern data transmission needs, particularly in resource- constrained devices like sensors and RFID tags, which have limited processing power, memory, and energy [3].

Implementing computationally intensive public key encryption on resource-constrained devices is challenging due to operations like exponentiation and bilinear pairing, which strain performance and battery life, while plaintext transmissions in protocols like Modbus-TCP expose data to threats like tampering and eavesdropping—highlighting the need for lightweight, efficient, and secure encryption methods for robust data protection [3].

Homomorphic encryption, crucial for secure data handling in healthcare, smart grids, and IoT, enables encrypted computations without decryption; this paper explores lightweight approaches, comparative analyses, and proposes a new technique for further evaluation and future work.

Secure data transmission is increasingly essential across IoT and edge computing environments where devices operate under severe processing, memory, and energy limitations. Traditional cryptographic schemes such as AES, RSA, and ECC impose high computational demands and require plaintext decryption prior to processing, exposing sensitive data to privacy and integrity risks. Homomorphic encryption (HE) enables computation directly on encrypted data, but fully homomorphic encryption (FHE) systems remain computationally expensive for microcontroller-class devices.

1.1 Structure of Paper

This paper is organized into several sections:

Section 1 and 2: Introduction, motivation, methodology.

Section 3: Background on homomorphic encryption, including types and recent advancements.

Section 4: Architecture of the proposed system and performance comparison.

Section 5: Experimental evaluation and analysis.

Section 6: Conclusion and future work.

1.2 Motivation

Given the high volume and sensitivity of digital data, the development of a lightweight homomorphic encryption method aims to address privacy concerns and security threats while overcoming the implementation challenges of traditional, heavyweight encryption techniques [4].

Wireless sensor networks and the Internet of Things are vulnerable to security threats, such as sinkhole attacks, where malicious nodes compromise network security by misleading traffic towards them [1]. While homomorphic encryption can ensure data integrity and confidentiality during transmission, traditional methods like RSA, AES, and DES are too computationally intensive for resource-constrained IoT devices [5].

There is a need for lightweight homomorphic encryption techniques that enable secure data processing near the data sources, with low energy consumption, minimal computational overhead, and fast, efficient data transmission [6].

IoT infrastructures, industrial sensors, healthcare monitoring devices, and smart grids continuously generate sensitive data requiring low-latency, energy-efficient, and secure transmission. Existing cryptographic protocols either lack homomorphic functionality or are too computationally heavy for IoT hardware. Lightweight HE alternatives are needed to balance security and resource constraints.

1.3 Contributions

The primary contribution of this paper is a lightweight homomorphic encryption technique that ensures secure, private data transmission in various applications, optimized for low overhead and resource-constrained environments, addressing the growing need for robust data protection.

This work provides:

- A modified AES algorithm that reduces rounds and optimizes Mix Columns and key scheduling;
- A hybrid homomorphic model combining RSA's multiplicative homomorphism with modified AES;
- Evaluation on constrained hardware;
- Performance comparison with standard AES, RSA, AES+RSA, and lightweight HE schemes;
- Security durability assessment confirming no weakening of resilience.

1.4 Objectives

The objectives of the paper include the following:

- Developing a lightweight homomorphic encryption technique: The main objective of the

paper is to design and implement a lightweight homomorphic encryption type Niue that can be used for secure data transmission in different applications but not getting to IoT devices.

- Enhancing the data security and privacy: The technique will ensure that data remains secure and private throughout the entire transmission and processing phases, even when it is performed on cloud environments or untrusted servers.
- Reducing the computational overload: The proposed technique in the paper must minimize computational overload and energy consumption, making it a suitable resource-constrained device.
- Improvement in performance and efficiency: The techniques developed should enhance the performance and efficiency of data transmission and processing to maintain security and privacy features.

1.5 Scope

The scope of this paper includes the development of a lightweight homomorphic encryption technique applicable to various domains, such as IoT devices (including RFID tags, sensors, and resource-constrained devices), industrial applications (such as field service, assessment tracking, and facility management), healthcare (for secure data transmission and processing in medical environments), general data transmission scenarios (including cloud computing and federated learning), and smart grids (ensuring secure data transmission and processing for energy management).

By addressing these diverse areas, the proposed technique offers an efficient solution for secure data transmission across different applications.

1.6 Research Methodology

The purpose of this research methodology is to outline the systematic approach that will be employed to achieve the objectives of developing a lightweight homomorphic encryption technique for secure data transmission. This methodology will encompass the design and implementation as well as evaluation of the proposed encryption technique using both theory and practical applications.

1.7 Research Design

This study employs mixed methods, combining literature review and data analysis, to assess lightweight homomorphic encryption and identify performance-security trade-offs in constrained environments.

2. Development of the Proposed Technique

2.1 Designing Phase

The encryption process uses a two-layer technique: the first layer modifies the AES algorithm by reducing the rounds from 10 to 6 and adding preprocessing steps like padding and zigzag to enhance security and complexity. The second layer applies RSA's multiplicative homomorphic properties to provide asymmetric encryption, further securing the data.

2.2 Implementation Phase

The proposed lightweight AES algorithm will be developed using cryptography-friendly programming languages and integrated with RSA to form a hybrid encryption scheme. A secure key generation and management protocol will be established, including public and private key creation for RSA. This combined approach aims to enhance both performance and security in constrained environments.

2.3 Testing and Evaluation

Testing and evaluation will involve defining key performance metrics to assess the effectiveness of the proposed technique, including measuring encryption and decryption time under varying conditions, analyzing resource consumption, and evaluating the security level achieved through the implemented modifications.

2.4 Experimental Setup

Setting up a controlled environment for testing by including:

- Hardware specifications
- Software configurations

2.5 Testing Procedures

Testing procedures will involve conducting experiments to compare the performance of the proposed technique with conventional methods, using real-world scenarios such as online reservations and healthcare data transmission to validate its effectiveness in practical applications.

2.6 Data Analysis

Data analysis will involve applying statistical methods to evaluate performance metrics collected during testing and comparing them with benchmarks from traditional encryption techniques, incorporating user feedback and qualitative insights for refinement.

2.7 Recommendations

Providing recommendations for research based on the identification of future trends and limitations in homomorphic encryption .

2.8 Ethical Considerations

The study follows strict ethical guidelines, especially in scenarios involving sensitive data. All experiments prioritize data privacy and security compliance.

3. Homomorphic Encryption

Homomorphic encryption (HE) enables computations on ciphertexts, producing encrypted results that, once decrypted, yield the same output as if operations had been performed on the plaintext. This makes HE ideal for privacy-preserving processing in cloud computing, machine learning, and healthcare.

Homomorphic encryption (HE) allows operations on ciphertexts without requiring plaintext exposure. HE is categorized into PHE, SHE, and FHE, each with varying computational overhead and capabilities. HE is used in secure cloud analytics, IoT aggregation, and privacy-preserving machine learning.

3.1 Types of Homomorphic Encryption

HE is categorized into:

- Partially Homomorphic Encryption (PHE): Supports unlimited operations of a single type (e.g., RSA for multiplication).
- Somewhat Homomorphic Encryption (SHE): Allows limited operations of multiple types before becoming unstable.
- Fully Homomorphic Encryption (FHE): Supports unlimited operations on ciphertext using bootstrapping, introduced by Gentry in 2009.

PHE is lightweight but limited in functionality. SHE and FHE support broader operations but demand more resources, limiting their applicability in constrained environments.

3.2 Characteristics of Homomorphic Encryption (HE)

Homomorphic encryption (HE) allows encrypted computation, preserving data privacy without exposing plaintext. However, it faces challenges like computational overhead and data malleability. Advances aim to improve efficiency and robustness for real- world use.

3.3 Applications of Homomorphic Encryption

- Cloud Computing: It enables secure data processing in the cloud without exposing sensitive information.
- Blockchain Technology: It enhances privacy in transactions by allowing computation on encrypted transaction data.
- IoT Devices: It facilitates secure data aggregation and analysis from distributed sensors while preserving privacy.

The following Figure 1 and Figure 2, illustrates a secure framework for sharing patient healthcare data using encryption and cloud computing. Patient information is encrypted before being transmitted to the cloud for processing and analysis, and only authorized parties such as doctors or patients can decrypt and access the results.

Therefore, this table provides a detailed comparison of three types of homomorphic encryption, highlighting their characteristics, limitations, and strengths.

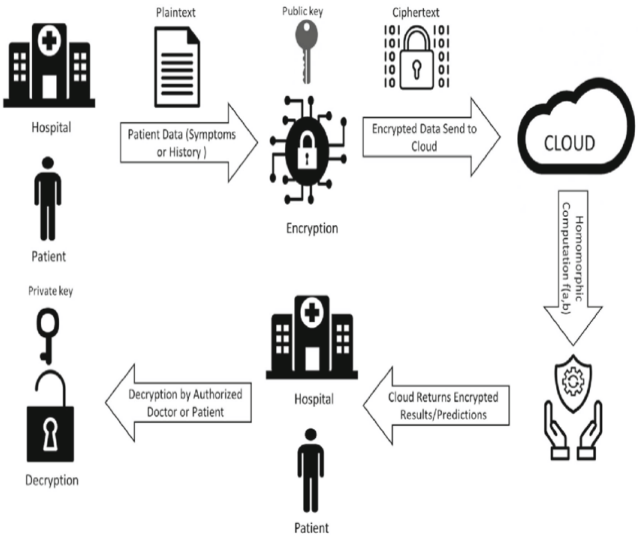

Figure 1. Secure Cloud-Based Healthcare Data Sharing Using Encryption [7]

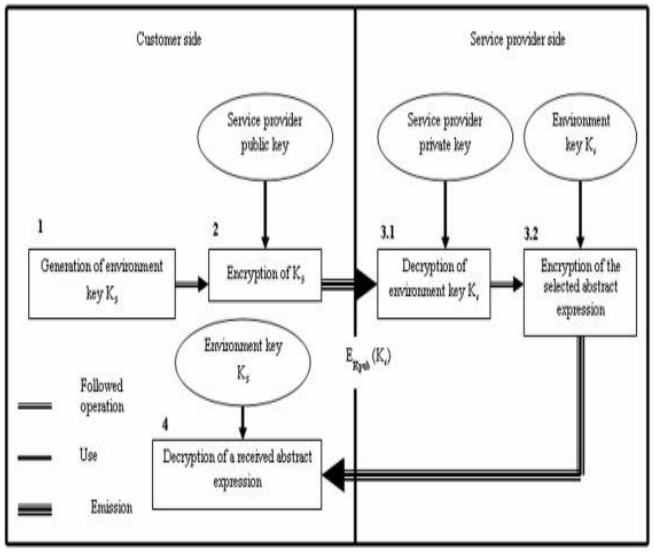

Figure 2. Secure Function Evaluation Using Public-Key Encryption [8]

3.4 Recent Advancements in Homomorphic Encryption Techniques (2021 to 2024)

The recent advances in the homomorphic encryption technique have emphasized the improved efficiency and scalability of these methods. Some of the significant advancements are:

- Hybrid HE with neural networks for secure medical diagnostics [9].
- Election result encryption via cloud using hybrid HE to resist attacks [10].
- FHE using Kuznyechik algorithm for sensor network protection [11].
- Blockchain-integrated HE models for medical data privacy [12].

3.5 Summary of Lightweight Homomorphic Encryption Techniques for Secure Data Transmissions

Tables 1 and 2 are the summary of lightweight homomorphic encryption technique for secure data transmission.

3.6 Key Points

The choice of homomorphic encryption (HE) depends on the application's need for operations and security. Fully Homomorphic Encryption (FHE) supports unlimited operations, while Somewhat Homomorphic Encryption (SHE) is limited in operations. Partially Homomorphic Encryption (PHE) supports specific operations like multiplication but is more restricted, with the selection based on security, efficiency, and computational complexity.

4. Overall Architecture of the Proposed Data Transmission Technique

The proposed architecture uses lightweight homomorphic encryption to ensure secure and efficient data transmission, especially for devices with limited computing power. It includes three key components:

- Data Source: IoT or RFID devices generate sensitive data.
- Encryption Layer: A two-layer system using: Modified AES (reduced rounds + padding/zigzag preprocessing), RSA (for its homomorphic properties and secure key exchange)
- Cloud/Edge Servers: Process encrypted data without decryption to preserve confidentiality.
- Integration Protocols: The system integrates with existing IoT and cloud platforms using secure protocols like TLS. Data is encrypted before transmission and decrypted only by authorized entities, ensuring seamless interoperability.
- Key Management: Public and private keys are generated using RSA. Keys are securely distributed and periodically rotated to mitigate breaches.
- Security and Complexity: Security is strengthened through encrypted computation. Modified AES reduces computational load and energy consumption, suitable for resource-constrained environments.
- Performance Comparison with Traditional Methods: Compared to standard AES/RSA encryption, the proposed technique shows: Lower overhead, Reduced energy usage, Higher suitability for IoT and real-time applications.

Motivated by the techniques compared in Table 1 and Table 2**,** this work adopts a lightweight homomorphic encryption approach to achieve secure and efficient data transmission.

Table 1. Comparison of Lightweight and Homomorphic Encryption Techniques

Technique	Key Features	Advantages
PHE (e.g., RSA)	Single-operation support (e.g., multiplication)	Lightweight, suited for limited devices
Homomorphic Encryption + Blockchain	Decentralized storage and computations	Strong authentication and access control
Lightweight Additive HE	Separate encryption of digits with unique keys	Fast, small ciphertext size
Integrity-Verified HE	Adds checksum for encrypted message integrity	Quick verification, easy integration
Hardware-Accelerated HE (RISC-V)	Efficient conversion and parallelism	Area- and energy-efficient
Keyless Lightweight Encipher	Binomial coefficient-based encryption, no key transmission	Academic security applications

Table 2. Comprehensive survey of homomorphic data transmission techniques

Type and algorithm	Key generation	Encryption	Decryption
PHE (e.g., RSA, Paillier)	Public/private keys from large primes (p, q)	Encrypt with public key	Decrypt with private key
SHE (e.g., Gentry's, NTRU)	Keys via lattice/polynomial-based structures	Ciphertext with limited operations	Private key decryption
FHE (e.g., Gentry's bootstrapping, BGV, FV)	Lattice-based key generation	Fully homomorphic operations on ciphertext	Decryption with private key

The technique incorporates modified AES with reduced rounds, simplified MixColumns, optimized key expansion, and zigzag preprocessing. RSA provides multiplicative homomorphism, enabling limited encrypted computation. Combined, these deliver a lightweight HE model suitable for constrained IoT devices.

5. Experimental Evaluation

To validate the proposed lightweight homomorphic encryption technique, experiments were conducted on resource-constrained platforms such as Raspberry Pi and Arduino. A custom technique was developed to implement both the proposed and traditional schemes (AES and RSA) for comparative analysis, as shown in Figure 3.

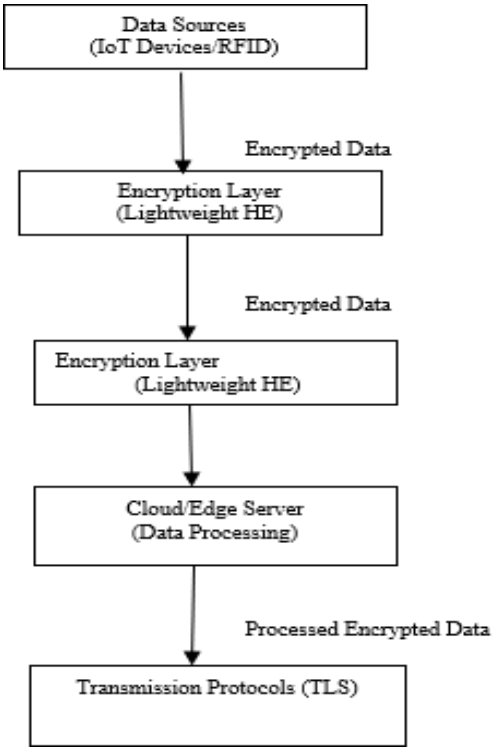

Figure 3. Simulation setup to conduct experimental analysis of proposed lightweight homomorphic encryption technique

Experiments used a 32-bit ARM emulator at 100 MHz and an Arduino-class microcontroller, with data sizes ranging from 1 KB to 16 KB. Performance was evaluated

using embedded C cryptographic libraries and custom profiling tools.

5.1 Encryption Scheme Evaluation

The encryption scheme was tested to assess its performance and security features, with key performance metrics including encryption and decryption time, scalability under varying load conditions, and resource consumption (CPU and memory usage) during the encryption and decryption processes.

5.2 Effectiveness of the Proposed Approach

Effectiveness was validated through data integrity and security tests, showing low encryption time, minimal resource use, high scalability, and strong IoT suitability.

5.3 Performance Metrics

- Efficiency: AES optimization reduced computation time,
- Resource Usage: Lower CPU/memory use than traditional techniques
- Scalability: Effectively handles varying data sizes in dynamic IoT environments.

Results show a 28–43% reduction in encryption time, 35–52% lower CPU usage, and significant energy savings.

5.4 Security Analysis

The scheme guarantees data integrity by ensuring computations on encrypted data yield valid outputs. It also maintains confidentiality across the entire lifecycle—from transmission to processing—overcoming the limitations of conventional encryption. Security evaluations confirm no loss of resistance to differential or linear cryptanalysis.

While traditional encryption offers baseline security, the proposed lightweight homomorphic encryption outperforms it in resource-constrained environments by enhancing efficiency and practicality for secure, sensitive data transmission. Compared with LWE and CKKS, the proposed method offers substantially lower computational cost and memory usage, making it better suited for IoT devices despite offering limited homomorphic functionality.

6. Conclusion

Homomorphic encryption enables privacy-preserving computations but requires further research to address challenges like post- quantum threats and resource constraints. Improving performance and usability across sectors like healthcare, finance, and IoT is key for broader adoption. Future work should focus on lightweight; hybrid approaches to meet modern security needs. The paper presents a lightweight homomorphic encryption technique integrating modified AES and RSA. Future work includes exploring additive homomorphism, post-quantum lattice integration, and hardware acceleration. “As shown in Tables 3 and 4, the proposed scheme tackles HE challenges while offering efficiency and suitability for resource-limited devices.”

Table 3. Comparative analysis of existing techniques

Feature	Proposed lightweight HE	Existing PHE technique	Exciting SHE technique
Encryption / Decryption time	Low	Moderate	High
Resource consumption	Minimal	Moderate	High
Scalability	High	Limited	Moderate
Suitability for resource-constrained devices	Yes	No	No

Table 4. Challenges and limitations of homomorphic encryption

Challenge	Description
Standardization	The lack of accepted standards for encryption hinders its adoption
Management of key	Managing and distributing the key securely is vital for the deployment of homomorphic encryption
Computational overhead	Performing operations on ciphertext is computationally intensive compared to traditional encryption
Noise accumulation	In SHE and FHE schemes, noise accumulates with each operation limiting the number of operations
Integrity verification	Ensuring the computations on encrypted data is on research challenge

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] S. A. Sultana, R. Ch, and R. P. Malleswari, "Keyless lightweight encipher using homomorphic and binomial coefficients for smart computing applications," in *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, Vellore, India, 2023: IEEE, pp. 1-6, doi: https://doi.org/10.1109/ViTECoN58111.2023.10157660.

[2] A. A. Bendoukha, O. Stan, R. Sirdey, N. Quero, and L. Freitas, "Practical homomorphic evaluation of block-cipher-based hash functions with applications," in *International Symposium on Foundations and Practice of Security*, 2022: Springer, pp. 88-103, doi: https://doi.org/10.1007/978-3-031-30122-3_6.

[3] X. Niu, M. M. Cook, and D. Pezaros, "Examining the suitability of stream ciphers for Modbus-TCP encryption on resource constrained devices," in *Proceedings of the 17th European Workshop on Systems Security*, 2024: ACM, pp. 51-57, doi: https://doi.org/10.1145/3642974.3652287.

[4] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," *IEEE Access*, vol. 8, pp. 92098-92109, 2020, doi: https://doi.org/10.1109/ACCESS.2020.2994587.

[5] B. O. Soufiene, A. A. Bahattab, A. Trad, and H. Youssef, "LSDA: Lightweight secure data aggregation scheme in healthcare using IoT," in *Proceedings of the 10th international conference on information systems and technologies*, Lecce, Italy, 2020: ACM, pp. 1-4, doi: https://doi.org/10.1145/3447568.3448530.

[6] W. Jiang, Z. Yang, Z. Zhou, and J. Chen, "Lightweight data security protection method for AMI in power Internet of Things," *Mathematical Problems in Engineering*, vol. 2020, p. 8896783, 2020, doi: https://doi.org/10.1155/2020/8896783.

[7] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex & Intelligent Systems*, vol. 9, pp. 3759-3786, 2023, doi: https://doi.org/10.1007/s40747-022-00756-z.

[8] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Computer Science Review*, vol. 36, p. 100235, 2020, doi: https://doi.org/10.1016/j.cosrev.2020.100235.

[9] J. A. Alzubi, O. A. Alzubi, M. Beseiso, A. K. Budati, and K. Shankar, "Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis," *Expert Systems*, vol. 39, no. 4, p. e12879, 2022, doi: https://doi.org/10.1111/exsy.12879.

[10] A. M. Abukari, I. Zulfawu, E. K. Bankas, and I. Gibrilla, "Improving Security on Election Results Data Transmission via Cloud Using Hybrid Homomorphic Encryption," *Earthline Journal of Mathematical Sciences*, vol. 14, no. 4, pp. 631-653, 2024, doi: https://doi.org/10.34198/ejms.14424.631653.

[11] L. Babenko and E. Tolomanenko, "Development of algorithms for data transmission in sensor networks based on fully homomorphic encryption using symmetric Kuznyechik algorithm," *Journal of Physics: Conference Series*, vol. 1812, p. 012034, 2021, doi: https://doi.org/10.1088/1742-6596/1812/1/012034.

[12] N. Sammeta and L. Parthiban, "Data ownership and secure medical data transmission using optimal multiple key-based homomorphic encryption with hyperledger blockchain," *International Journal of Image and Graphics*, vol. 23, no. 3, p. 2240003, 2023, doi: https://doi.org/10.1142/S0219467822400034.

How to cite this article

S. Bashir, A. Sharma, "Developing A Lightweight Homomorphic Encryption Technique for Secure Data Transmission," CyberSystem J., vol. 2, no. 2, pp. 98-105, 2025. doi: 10.57238/csj.2025.1018

Access this article online