International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 5, Sep-Oct 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Enhancing Cloud Data Security Using Homomorphic Encryption Techniques

Gopal Prasad Sharma

Associate Professor, Purbanchal University School of Science & Technology (PUSAT), Biratnagar, Nepal

ABSTRACT

As cloud computing completely changes how companies store and process data, data security has become more important. When we use standard encryption methods in the cloud, which don't work well with the unique restrictions of this setting, we often end up with data breaches and more points of vulnerability. Homomorphic Encryption (HE), which lets us do calculations on encrypted data without showing the data itself, is a game-changing option. The article discusses the operation of homomorphic encryption and its potential to enhance cloud security, data protection, and trust. There are several trends that could potentially enhance the security of homomorphic encryption in the future, as cloud data security is limited. Real-life case studies and applications are used in this piece to show and discuss about how this cutting-edge cryptographic method works in the real world. The future of cloud data security will be significantly influenced by heteromorphic encryption.

KEYWORDS: *Homomorphic Encryption, Cloud Computing, Data Security, Privacy, Compliance*

How to cite this paper: Gopal Prasad Sharma "Enhancing Cloud Data Security Using Homomorphic Encryption Techniques" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-5, October 2024, pp.940-946, URL: www.ijtsrd.com/papers/ijtsrd70464.pdf

IJTSRD70464

1. INTRODUCTION

Cloud computing has revolutionised data storage and administration. Distributes computer services over the Internet ("the cloud") to give consumers on-demand access to many resources [1]. These services include servers, storage, databases, networking, software, analytics, and intelligence. This paradigm allows faster scalability, lower hardware maintenance costs, and better teamwork across locations. Cloud computing's efficiency, scalability, and agility make it important to today's IT architecture. Cloud storage can improve data backup, content distribution, and disaster recovery for businesses [2]. Cloud-hosted ERP and CRM applications are common. Remote work, collaboration, and data access from anywhere are all benefits of cloud storage. Many cloud providers also offer advanced analytics solutions to help companies acquire data insights. With the rise of cloud computing, data security is more vital. Cloud computing has security vulnerabilities. Cloud data is susceptible to data breaches, ransomware, and unauthorised access [3]. Numerous newspapers have reported that data breaches that revealed personal information have cost many companies money and reputation. The law and the correct course of action are to safeguard sensitive data, as cloud data may be required to adhere to regulations. Cloud data protection is indispensable in light of these concerns. In order to safeguard data, organisations should establish rigorous security protocols.

Deep Neural Networks (DNNs) made it famous for processing big, unstructured data sets better than standard machine learning.

2. Homomorphic Encryption

Homomorphic encryption, a complex cryptographic approach, permits calculation on encrypted data without revealing the plaintext [4]. This unique function lets users instantaneously add and multiply encrypted data, resulting in an encrypted result that matches the original data's output. Cloud computing, which processes and stores sensitive data remotely, requires this feature for data privacy. Homomorphic encryption requires meaningful computations and confidentiality. Allowing computations on ciphertexts protects sensitive data in untrusted environments. Cloud computing is difficult because customers must trust third-party providers with sensitive data.

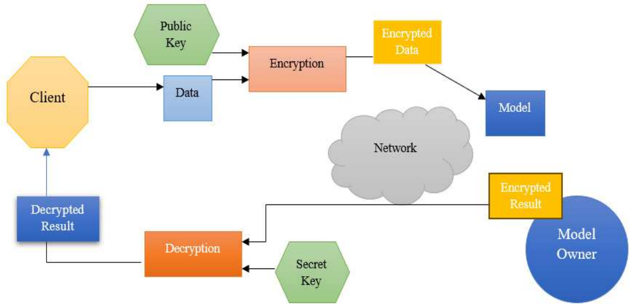


Figure 1 Homomorphic Encryption (Source: Self-created)

2.1. Types of Homomorphic Encryption

Based on the scope of data manipulations, homomorphic encryption has three main types:

Partially Homomorphic Encryption (PHE): This type adds or multiplies ciphertexts but not both. PHE is used in RSA encryption, which multiplies encrypted data. PHE provides some security for certain applications, but complicated computations are limited by its constraints [5].

Somewhat Homomorphic Encryption (SHE): SHE methods allow limited ciphertext addition and multiplication. This kind is more flexible than PHE but limited by the amount of processes before the ciphertext gets too noisy to decrypt. SHE schemes like Brakerski-Gentry-Vaikuntanathan (BGV) allow moderate activities while ensuring security [6].

Fully Homomorphic Encryption (FHE): FHE is the most powerful homomorphic encryption, providing limitless ciphertext addition and multiplication. Secure data analysis, machine learning, and other applications benefit from this ability to perform complex computations on encrypted data [7]. CraigGentry introduced the first workable FHE technique in 2009, a cryptographic breakthrough.

2.2. Working of Homomorphic Encryption

Homomorphic encryption uses numerous ideas and methods to secure and function encrypted data processing.

Basic Principles

Encryption: We encrypt plaintext with a public key first. By converting plaintext to ciphertext, encryption makes data practically unreadable without the decryption key.

Computation on Ciphertext: Use ciphertext for computations without decryption. The methods vary by homomorphic encryption method, but addition and multiplication are usually included.

Decryption: When computations are complete, send the ciphertext to the data owner so they can decode it with a private key.

Algorithms Involved

Homomorphic encryption works with several algorithms, each with its own security and processing efficiency. FHE uses Learning With Errors (LWE) and other lattice-based encryption methods because they withstand quantum attacks. Famous techniques for partially or completely homomorphic encryption include integer factorisation and elliptic curve cryptography.

2.3. Overview of the Encryption and Decryption Processes

Encryption Process

- The user generates a public/private key pair.
- The plaintext data is encrypted using the public key, resulting in ciphertext.
- The ciphertext is sent to a cloud service or another party for processing.

Computation on Encrypted Data

- The cloud service performs the designated operations on the ciphertext, yielding a new ciphertext that represents the result of the computation.

Decryption Process

- The computed ciphertext is sent back to the data owner.
- The data owner decrypts the ciphertext using the private key, exposing the end result that matches the plaintext action.
- Thus, homomorphic encryption secures cloud data, allowing organisations to use cloud computing while protecting sensitive data. Homomorphic encryption research promises to improve efficiency and expand its use in healthcare and finance.

3. Current State of Cloud Data Security

3.1. Overview of Traditional Encryption Methods

Cloud encryption protects sensitive data against unauthorised access. The majority of encryption techniques are symmetric or asymmetric.

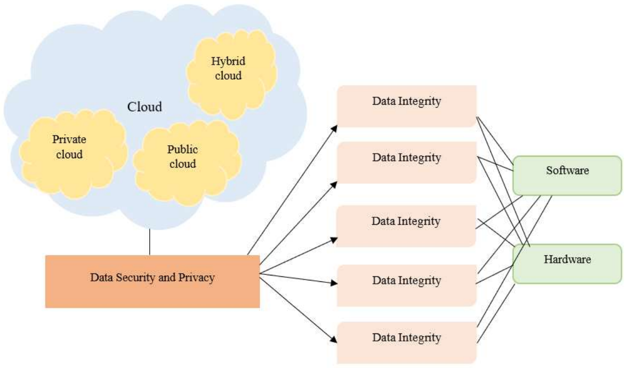


Figure 1 Cloud Data Security (Source: Self-created)

Symmetric Encryption: Data is encrypted and decrypted using the same key in symmetric encryption. Sender and receiver must share a secret key to encrypt and decrypt messages. Symmetric algorithms like AES and DES are well-known. Symmetric encryption is more efficient at processing large amounts of data quickly and using little computational power [8]. The issue is distributing and managing encryption keys safely. A key compromise threatens the entire system.

Asymmetric Encryption: Asymmetric encryption uses public and private keys. Private keys are kept secret and used for decoding, but public keys can be used to encrypt data. RSA and ECC are used in asymmetric encryption [9]. This strategy increases security by not transmitting the private key. It is slower and less efficient than symmetric encryption, making it unsuitable for real-time encryption of large volumes of data. In cloud computing, even the strongest encryption systems have restrictions. Data decryption before processing is a major issue. Unaffiliated third parties' cloud-stored private data may be required.

Safe key management may be hampered by standard encryption systems, hindering user collaboration and data interchange.

3.2. Existing Security Challenges

Taking sensitive data to the cloud poses security issues for businesses.

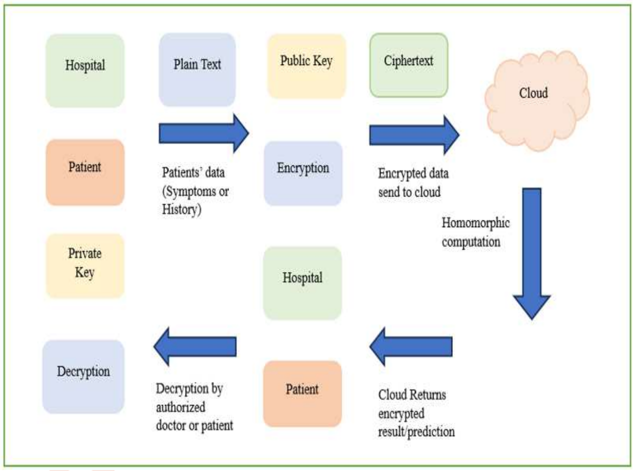
- ➢ Preventing data leaks is cloud providers' primary priority. Cloud security vulnerabilities allow thieves to steal critical data. Data leaks can damage reputation, financial accounts, and legal status. Cloud data requires improved protection after high-profile attacks on major organisations.
- ➢ Theft of sensitive data by thieves is another concern. Effective attackers may be able to compromise cloud services due to weak authentication [10]. Once in, they might take data or alter it to compromise data integrity, making systems more vulnerable to assaults. Businesses should use role-based access limitations and multi-factor authentication to mitigate these dangers.
- ➢ Integrity determines cloud data reliability. Corruption or illegal data alterations can disrupt operations and cause blunders. Keep extensive audit records and use checksums or hashes to discover and fix integrity issues.
- ➢ Banking and healthcare have strict data security and privacy requirements. Companies handling personal data must obey HIPAA and GDPR. Infractions can lead to fines and reputation damage. Cloud providers prioritise these requirements despite operational complexity [11].

Organisations should protect cloud data with access limits and traditional encryption. Due to the limits of traditional encryption methods, especially for encrypted data, homomorphic encryption is growing in popularity. These innovations let businesses securely analyse cloud data and obtain insights. Modern cyberthreats outgrow traditional cloud data encryption. Companies must improve their security to protect personal data and meet evolving standards.

4. Benefits of Using Homomorphic Encryption in Cloud Security

Homomorphic encryption improves cloud data security.

Homomorphic Encryption (HE) enables encrypted data computations without decryption, improving cloud service providers' data privacy, security, and compliance.


Hospital
Plain Text
Public Key
Ciphertext
Cloud
Patient
Patients' data (Symptoms or History)
Encryption
Encrypted data send to cloud
Homomorphic computation
Private Key
Hospital
Decryption
Decryption by authorized doctor or patient
Patient
Cloud Returns encrypted result/prediction

Figures 3 Homomorphic Encryption in Cloud Security (Source: Self-created)

Data Privacy and Confidentiality

Data privacy and processing secrecy are important benefits of homomorphic encryption. Decrypting sensitive data before computation is typical in conventional cloud systems [12]. Privacy risks arise with unencrypted data, especially with third-party cloud providers. To circumvent this, homomorphic encryption encrypts data during computation. To better assess and plan therapy, healthcare organisations might encrypt sensitive patient data before transferring it to the cloud. Without accessing medical records, the cloud provider can utilise homomorphic encryption to perform machine learning or statistical research on this encrypted data. Only authorised people with the decryption key can read the encrypted results provided to the organisation. Healthcare, finance, and government handle sensitive data and require this competence

[13]. Data is protected from breaches and privacy compliance throughout its processing lifecycle with homomorphic encryption.

Secure Computation in the Cloud

Homomorphic encryption revolutionises secure computing on encrypted data. User trust is needed because cloud providers manage unencrypted data in traditional systems [14].

Trust can be misplaced, leaving organisations vulnerable to significant security breaches. Cloud providers with homomorphic encryption can handle sensitive data. This secure computation technique helps organisations use cloud computing's scale and flexibility without data security concerns. The bank can encrypt transaction records before transferring them to a cloud provider for analysis. Without transaction specifics, the cloud service can compute and identify fraud patterns. The institution's secrecy prevents unauthorised users from decrypting results. Secure computing gives companies and cloud service providers trust by preventing data theft [15]. Companies use homomorphic encryption to reduce risk while outsourcing data analysis and processing to the cloud.

Compliance and Regulatory Benefits

HIPAA and the GDPR require organisations to follow all data protection rules. Reputational, legal, and financial consequences may result from inability to comply [16]. Homomorphic encryption improves compliance. Company commitment to consumer privacy and security can be shown by data encryption. This encryption technique meets data processing, retention, and access requirements. Companies must use technology to protect personal data under GDPR. Homomorphic encryption prevents data breaches and verifies compliance. HIPAA-covered healthcare organisations can protect patient data during processing via homomorphic encryption [17]. Companies can simplify data exchange agreements with third-party cloud providers using homomorphic encryption. Companies are able to comply with regulations by regulating the access of sensitive data and the timing of its release.

Reduced Risk of Data Breaches

Data breaches are a major cloud risk for enterprises. High-profile incidents show that hackers can attack even the most reliable cloud systems [18]. As more companies store sensitive data on the cloud, the risk of unlawful access and data exfiltration increases.

Homomorphic encryption protects encrypted data from cloud provider server compromises. If an attacker breaches cloud computing, they cannot decipher or access the data stored there because all computations employ ciphertext. Data breaches are much less likely when unencrypted data is blocked. With homomorphic encryption, monitoring and access controls can be added to reduce unauthorised access. Layered security using homomorphic encryption, strong authentication, and authorisation can improve data protection [19]. A corporation that safeguards sensitive data against data breaches is more trusted by customers, stakeholders, and regulatory bodies. Businesses that prioritise data security and deploy cutting-edge encryption are more likely to retain customers and partners.

5. Implementation Challenges and Considerations

Although difficult, HE can secure cloud data. Companies using this cutting-edge encryption face performance, technical complexity, and scalability concerns. Companies considering homomorphic encryption in cloud infrastructures should address these issues.

Performance Issues

Computer computational cost is a big issue with homomorphic encryption. HE encryption and decryption need higher system resources. When encrypting data, modular and lattice-based calculations might increase processing load. Time-sensitive applications cannot use homomorphic encryption due to its computational cost [20]. Big data analytics and machine learning may suffer from HE. These jobs require quick huge dataset computations. Decryption, processing, and encryption can slow an organization's economic and market response. Type impacts homomorphic encryption. Fully Homomorphic Encryption (FHE) has the most operational flexibility but the highest computational overhead [21]. FHE may outperform SHE, although both limit operations. Before using homomorphic encryption, companies should assess performance and operational limits.

Technical Complexity

Homomorphic encryption in cloud infrastructures is technologically challenging. Integrating HE into security systems can be difficult for organisations without advanced cryptography skills.

Old approaches may not work with homomorphic encryption in cloud architecture [22]. To implement HE, companies may need to alter their data processing systems. This integration may be complicated by data storage, access limitations, and processing pipeline adjustments.

To implement efficiently, you must master homomorphic encryption, a subfield of advanced cryptography. Investing in personnel training or higher education experts is not always feasible. Lack of competent staff and readily available resources may limit homomorphic encryption deployment.

To balance security and performance, choose the correct homomorphic encryption algorithm. In order to identify the most effective algorithm, businesses must implement multiple evaluations. Algorithms determine encryption performance.

Scalability Concerns

Scale homomorphic encryption for large datasets and high transaction volumes. Scaling HE systems without sacrificing performance is essential as data grows exponentially.

Homomorphic encryption generates large ciphertexts. Data bloat complicates processing, transit, and storage [23]. Larger encrypted datasets require more work, which could slow data processing.

Homomorphic encryption computational requirements increase with data. The performance cost from HE may be prohibitive for businesses that expect their calculations on vast datasets to become more complicated. This issue may require more expensive processing resources or specialised equipment.

Daily workloads vary, and many organisations operate in unexpected environments. Flexible and efficient, homomorphic encryption solutions manage any workload [24]. Complexity makes this adaptability difficult in higher education, but it's essential for data processing enterprises.

6. Case Studies and Real-World Applications

IBM and the Helios Voting System

IBM's Helios voting system demonstrates homomorphic encryption.

Helios, a free, open-source electronic voting system, lets voters inspect ballots and protect them with homomorphic encryption [25]. This system encrypts votes before counting data. This method lets election officials calculate final vote totals without seeing individual votes. Helios' homomorphic encryption improves voter privacy and confidence in elections.

The mechanism is transparent, allowing electors to observe the results and rest assured that their decisions will not be disclosed. However, computational cost and cryptography-specific skills have been detected during implementation, requiring careful preparation and resource distribution.

Microsoft Azure and Confidential Computing

Microsoft Azure's Confidential Computing program uses homomorphic encryption. This initiative's secure enclaves protect data during processing. Homomorphic encryption lets organisations calculate sensitive data in Azure without Microsoft or others accessing it. Healthcare and financial companies utilise this technology to securely evaluate private datasets. Azure's Confidential Computing lets healthcare businesses evaluate patient data in accordance with HIPAA. Trust in cloud solutions has increased as data breaches have decreased. Still, businesses struggle to integrate HE into their processes and train personnel on the technology.

NVIDIA and Secure Machine Learning

In federated learning, NVIDIA has considered homomorphic encryption to secure sensitive data. NVIDIA's encrypted data computations enable sensitive data machine learning model training [26]. This technology lets banks securely evaluate transaction data to detect fraud. The findings show improved data privacy and security, helping organisations meet laws. Training models using encrypted input requires updating algorithms and hardware due to performance issues.

Analysis of Outcomes

The implementation of homomorphic encryption in these case studies has yielded significant benefits, including:

- By keeping data encrypted during processing, organizations can protect sensitive information from unauthorized access and potential breaches.
- Organizations can better meet legal and regulatory requirements, such as GDPR and HIPAA, by ensuring that sensitive data remains confidential throughout its lifecycle.
- In systems like Helios, the transparent nature of HE fosters trust among users, assuring them that their data is secure and handled appropriately.

However, challenges remain that organizations must navigate:

Computational Overhead: The performance impact of homomorphic encryption can be significant, leading to increased processing times and the need for more powerful computing resources.

Technical Complexity: Integrating HE into existing systems often requires specialized knowledge and skills, which may necessitate additional training for staff or hiring new personnel.

Scalability Issues: As data volumes grow, the scalability of homomorphic encryption solutions can become a concern, requiring organizations to develop strategies to manage larger datasets efficiently.

7. Future Trends and Developments

Recently developed theory and practice make HE more practical and efficient in many situations. The main focus of HE computational cost researchers is algorithm optimisation. Several homomorphic encryption methods use lattice-based cryptography for efficiency and security. Enhancing bootstrapping in FHE expedites and realisticizes encrypted calculations for practical applications. Hybrid models that combine homomorphic encryption with other cryptographic methods are also rising, providing a more balanced approach that addresses each algorithm's weaknesses. As these advances occur, homomorphic encryption could dramatically impact cloud security. HE could transform cloud data security and privacy, according to predictions. New legislation and data security concerns may make homomorphic encryption essential for cloud computing security.

Companies may now access essential data without disclosing it, making data management safer and more private. This functionality helps organisations comply with GDPR and HIPAA by showing clients their data is secure. With the rise of cloud services, security must be strong. The field of homomorphic encryption is developing secure multi-party computations that can decrypt encrypted data without revealing the inputs. As more is comprehended about homomorphic encryption, it should become feasible for the protection of cloud and internet data.

8. Conclusion

Homomorphic encryption revolutionises cloud data security. As more companies use cloud services to store and process data, strong security has always been important. Homomorphic encryption allows calculations on encrypted data, preserving anonymity and allowing data analysis. Homomorphic encryption improves data privacy, legal compliance, and secure calculations without exposing sensitive information, according to its analysis. Computing overhead, technological complexity, and scalability difficulties may develop during HE implementation. Organisations must overcome various challenges to use homomorphic encryption in cloud security. Homomorphic encryption will underpin secure cloud computing, making cloud data security brilliant. With this innovative technique, organisations may protect sensitive data and build trust with clients and partners. As we move towards a data-driven future, homomorphic encryption in cloud security frameworks will protect data and enable secure, collaborative data-driven decision-making.

9. Reference

[1] M. M. S. Altaee and M. Alanezi, "Enhancing cloud computing security by Paillier homomorphic encryption," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1771-1779, 2021.

[2] S. A. Khan, R. K. Aggarwal, and S. Kulkarni, "Enhanced homomorphic encryption scheme with PSO for encryption of cloud data," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 2019, pp. 395-400.

[3] M. Faiz, N. Fatima, R. Sandhu, M. Kaur, and V. Narayan, "Improved homomorphic encryption for security in cloud using particle swarm optimization," *Journal of Pharmaceutical Negative Results*, pp. 4761-4771, 2022.

[4] A. A. Alqarni, "A secure approach for data integration in cloud using Paillier homomorphic encryption," *Journal of Basic and Applied Sciences*, vol. 5, no. 2, pp. 15-21, 2021.

[5] N. Almoysheer, M. Humayun, and N. Z. Jhanjhi, "Enhancing cloud data security using multilevel encryption techniques," *Turkish Online Journal of Qualitative Inquiry*, vol. 12, no. 3, 2021.

[6] B. Seth, S. Dalal, and R. Kumar, "Hybrid homomorphic encryption scheme for secure cloud data storage," *Recent Advances in Computational Intelligence*, pp. 71-92, 2019.

[7] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing," *International Journal of Intelligent Networks*, vol. 3, pp. 16-30, 2022.

[8] S. Mittal, P. Jindal, and K. R. Ramkumar, "Data privacy and system security for banking on clouds using homomorphic encryption," in *2021 2nd International Conference for Emerging Technology (INCET)*, 2021, pp. 1-6.

[9] A. Singh and S. Sharma, "Enhancing data security in cloud using split algorithm, Caesar cipher, and Vigenere cipher, homomorphism encryption scheme," in *Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018*, Springer Singapore, 2019, pp. 157-166.

[10] K. A. Kumari, A. Sharma, C. Chakraborty, and M. Ananyaa, "Preserving health care data security and privacy using Carmichael's theorem-based homomorphic encryption and modified enhanced homomorphic encryption schemes in edge computing systems," *Big Data*, vol. 10, no. 1, pp. 1-17, 2022.

[11] S. J. Mohammed and D. B. Taha, "From cloud computing security towards homomorphic encryption: A comprehensive review," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1152-1161, 2021.

[12] I. Sudha and R. Nedunchelian, "A secure data protection technique for healthcare data in the cloud using homomorphic encryption and Jaya–Whale optimization algorithm," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 10, no. 06, p. 1950040, 2019.

[13] C. Rupa, Greeshmanth, and M. A. Shah, "Novel secure data protection scheme using Martino homomorphic encryption," *Journal of Cloud Computing*, vol. 12, no. 1, p. 47, 2023.

[14] S. Ali, S. A. Wadho, A. Yichiet, M. L. Gan, and C. K. Lee, "Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing," *Egyptian Informatics Journal*, vol. 27, p. 100519, 2024.

[15] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat, and M. U. Ali, "Enhanced security in cloud computing using neural network and encryption," *IEEE Access*, vol. 9, pp. 145785-145799, 2021.

[16] C. Regueiro, I. Seco, S. De Diego, O. Lage, and L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," *Information Processing & Management*, vol. 58, no. 6, p. 102745, 2021.

[17] M. A. Hossain and M. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *International Journal of Computers and Applications*, vol. 44, no. 5, pp. 455-464, 2022.

[18] M. Joseph and G. Mohan, "Design a hybrid optimization and homomorphic encryption for securing data in a cloud environment," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 9, no. 4, pp. 387-395, 2022.

[19] A. S. Sawant, "Enhancing encryption in cloud computing and reducing energy usage by using PSO-ALO algorithm to improve homomorphic encryption technique," Ph.D. dissertation, Dublin, National College of Ireland, 2022.

[20] V. Biksham and D. Vasumathi, "A lightweight fully homomorphic encryption scheme for cloud security," *International Journal of Information and Computer Security*, vol. 13, no. 3-4, pp. 357-371, 2020.

[21] G. Prabu Kanna and V. Vasudevan, "A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data," *Cluster Computing*, vol. 22, no. Suppl 4, pp. 9561-9569, 2019.

[22] R. Sendhil and A. Amuthan, "A descriptive study on homomorphic encryption schemes for enhancing security in fog computing," in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 2020, pp. 738-743.

[23] Y. Ameur and S. Bouzefrane, "Handling security issues by using homomorphic encryption in multi-cloud environment," *Procedia Computer Science*, vol. 220, pp. 390-397, 2023.

[24] P. Thangavel, P. S. A. Mary, M. M. RameshKannan, and K. Deiwakumari, "Enhancing data security in multi-cloud settings with homomorphic encryption: Concepts, uses, and obstacles," *Educational Administration: Theory and Practice*, vol. 30, no. 4, pp. 7347-7353, 2024.

[25] A. Murugesan, B. Saminathan, F. Al-Turjman, and R. L. Kumar, "Analysis on homomorphic technique for data security in fog computing," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, p. e3990, 2021.

[26] P. K. Rani, S. Sathiya, S. Sureshkumar, and B. A. Kumar, "Enhancing cloud security with hybrid encryption," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1445-1450.