Review of Computer Engineering Research
2024 Vol. 11, No. 3, pp. 130-139
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/76.v11i3.3955
© 2024 Conscientia Beam. All Rights Reserved.

Overview of homomorphic encryption technology for data privacy

Qiang Chen[1,2]
Huixian Li[1,3]
Suriyani Ariffin[1+]
Nur Atiqah Sia Abdullah[1]

[1]*College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.*
[1]*Email: suriyani@uitm.edu.my*
[1]*Email: atiqah@tmsk.uitm.edu.my*
[2]*Dongguan City University, No. Wenchang Road, Liaobu Town, Dongguan City, Guangdong Province, China.*
[1,2]*Email: 48044244@qq.com*
[3]*College of Financial Technology, Hebei Finance University, Baoding, Hebei, China.*
[1,3]*Email: 153193723@qq.com*

(+ Corresponding author)

Article History
Received: 24 June 2024
Revised: 27 September 2024
Accepted: 10 October 2024
Published: 25 October 2024

Keywords
Big data
Homomorphic encryption
Privacy preservation
Cloud computing
Full homomorphic encryption
Partial homomorphic encryption.

ABSTRACT

This study examines the overview of homomorphic encryption technology for data privacy. In the era of big data, the growing need to utilize vast amounts of information while ensuring privacy and security has become a significant challenge. Homomorphic encryption technology has gained attention as a solution for privacy-preserving data processing, allowing computations on encrypted data without exposing sensitive information. This study introduces the concept of data privacy preservation and explores the evaluation of homomorphic encrypted technology. The focus is on analyzing both partial and full homomorphic encryption methods, highlighting their respective characteristics, evaluation criteria, and the current state of research. Partial homomorphic encryption supports limited operations, while full homomorphic encryption enables unlimited computation on encrypted data, though both face challenges related to computational overhead and efficiency. Additionally, this paper addresses the ongoing issues and limitations associated with homomorphic encryption, such as its complexity, large encryption volumes, and difficulties in handling large-scale datasets. Despite these challenges, researchers continue to refine the technology and expand its applications in cloud computing, big data analytics, and privacy-preserving computing environments. This study also discussed potential future research avenues aimed at improving the scalability, efficiency, and security of homomorphic encryption to support broader, real-world applications. Ultimately, homomorphic encryption is positioned as a key enabler for secure data utilization in an increasingly privacy-conscious digital landscape.

Contribution/Originality: This study provides a comprehensive analysis of partial and full homomorphic encryption, focusing on their evaluation metrics and limitations. Unlike previous works, it highlights the specific challenges of applying these technologies in large-scale big-data environments and proposes future research directions to overcome these barriers.

1. INTRODUCTION

In the era of big data, Internet user data has shown explosive growth in both type and scale, and these data have high value. However, the use of data also has privacy implications. Privacy leakage will affect individual rights and interests, but it will also have negative consequences for society. Privacy-Preserving has become particularly important in the era of big data. In addition to safeguarding individual rights and interests, protecting privacy also plays a crucial role in maintaining social stability and development. How to provide privacy preservation for sensitive user information that may be disclosed? In recent years, this is also the focus of academic and industrial attention.

In order to protect privacy, based on big data security protection technology, big data encryption schemes in different scenarios of big data environments are implemented. With strong applicability, encryption technology can be adopted to ensure data security. Encryption technology is one of the most effective means to ensure data security. If the information is more important during ordinary data transmission, you can encrypt it and transmit the ciphertext, preventing immediate access to the original data even if intercepted in the middle. Although the traditional encryption system can ensure the security of long-term storage of data, it cannot analyze and calculate the encrypted data because it depends on the sharing of the key between the two parties exchanging encrypted information, and the decryption of the data leads to privacy problems. Homomorphic encryption [1] is an effective technology to protect user privacy. It allows a third party to operate on encrypted data without decrypting it in advance, and the result obtained is the same as that obtained in plaintext. Therefore, the nature of homomorphic encryption also makes it can be used in the fields of outsourced computing services, big data analysis, and distributed storage. In recent years, homomorphic encryption technology has become a hot research direction of privacy preservation, and is being continuously optimized and broken through, and is gradually applied in cloud computing and privacy computing scenarios.

2. PRIVACY PRESERVING

2.1. Overview of Privacy Preserving

Data privacy refers to the protection of an individual's personal information, behavioral data, and other sensitive data. This data can include personally identifiable information, financial information, medical information, social media activity, emails, communications records, location data, and more. Data privacy content usually includes data collection, data storage, data use, data sharing and data destruction.

Privacy Preserving in the era of big data faces many challenges, the most important challenges include [2]:

2.1.1. Transparency of Data Collection and Use

In the era of big data, organizations and businesses widely collect and use data, and excessive collection of personal information may increase the risk of data breach or abuse. It is difficult for people to master their privacy rights, and organizations and businesses should collect personal information only when necessary and clearly state the purpose of collection and how it will be used.

2.1.2. Security of Data Processing

Cloud servers stores a large amount of data, relying on cloud computing platforms to ensure the privacy of user data. The credibility of these platforms greatly influences data security. Big data platform operation and maintenance managers may abuse or misuse the disclosure right of users' private data, damaging the confidentiality, integrity, and availability of user information or information systems. Therefore, protecting personal information from unauthorized access, use, or disclosure requires the use of reasonable technical and physical security measures.

2.1.3. Complexity of Data Sharing and Exchange

In the era of big data, data sharing and exchange involve the risk of privacy disclosure, and personal identity should be effectively anonymized or desensitized to reduce the risk of personal privacy disclosure.

2.2. Privacy Preserving Related Technologies

Data privacy preservation is the process of ensuring that such data is not accessed, used, or disclosed without authorization. With the rapid development and wide application of big data, cloud computing, and mobile Internet, business and user data are facing serious privacy leakage problems. The diversity of big data lead to multi-source data fusion, increasing the risk of privacy disclosure. The traditional passive privacy preservation technology, the outsourcing of storage and computing, makes the data generator lose the right to know and control the data. At present, data privacy preservation technologies usually include data anonymization, data desensitization, data encryption, differential privacy, and so on [2]. A Privacy Preserving technology is shown in Table 1.

Table 1. Privacy preserving technologies.

Privacy preserving technology	Description	Methods
Anonymization technology	The process of removing identifying elements from the data to prevent re-identification of the data subject.	● K-Anonymity ● L-diversity ● Differential privacy (DP)
Data desensitization technology	Some sensitive information is deformed by desensitization rules to achieve reliable protection of sensitive privacy data.	● Static data desensitization ● Dynamic data desensitization
Data encryption technology	Through mathematical algorithms, the plaintext data is converted into ciphertext data, and the original data can be restored only through the key technology.	● Homomorphic encryption (HE) ● Secure multi-party computing (SMPC) ● Federated learning (FL)

3. HOMOMORPHIC ENCRYPTION

3.1. Overview of Homomorphic Encryption

Homomorphic encryption, first introduced by Rivest, et al. [1] is a cryptographic technique that enables computations on encrypted data without the need for decryption. Homomorphic encryption ensures that the result of performing operations on encrypted data and then decrypting it is equivalent to performing the same operations on unencrypted data, according to the computational complexity theory. In homomorphic encryption schemes, E is the encryption algorithm function, M is the set of all possible messages, and m1 and m2 are subsets of M. If one of the conditions in Equations 1 or 2 is satisfied, the scheme is considered either an additive or multiplicative homomorphism.

$$E(m_1) + E(m_2) = E(m_1 + m_2), \forall m_1, m_2 \in M \qquad (1)$$

$$E(m_1) \times E(m_2) = E(m_1 \times m_2), \forall m_1, m_2 \in M \qquad (2)$$

Homomorphic encryption schemes consist of a key generation algorithm, an encryption algorithm, decryption algorithm, and an additional evaluation algorithm [1]. These schemes not only perform basic encryption operations but they also enable various computations directly on ciphertext without requiring decryption at each step. This reduces communication costs and shifts computational tasks, effectively balancing the workload across different parties. Furthermore, homomorphic encryption ensures that only the final result is decrypted, not the intermediate ciphertext, enhancing information security. The working principle of homomorphic encryption is shown in the Figure 1.

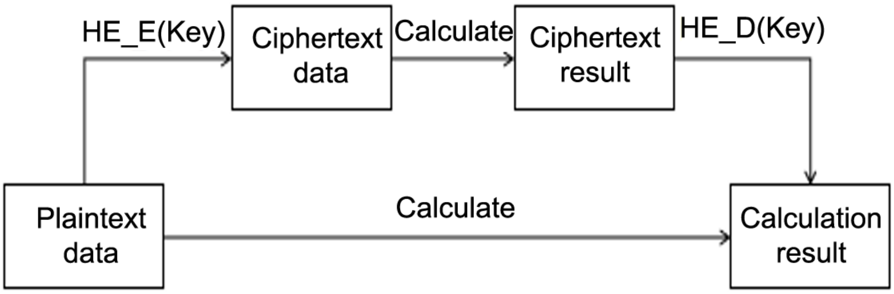

Figure 1. Homomorphic encryption processing.

Source: Gentry [3] and ElGamal [4].

1) Homomorphic encryption stage: the data to be processed needs to be encrypted using an encryption algorithm. This usually involves encrypting the data using a public-key encryption algorithm to generate ciphertext.
2) Calculation processing stage: various calculation operations can be performed on the ciphertext, such as addition, multiplication, comparison, etc. The ciphertext perform these operations, eliminating the need for decryption to plaintext.
3) Result extraction stage: After the calculation is completed, the ciphertext can be extracted from the obtained results and decrypted into plaintext. This process usually requires decryption using a private key.

3.2. Type of Homomorphic Encryption

As machine learning gains tractions, the cryptography community persists in enhancing and innovating homomorphic encryption, while the security concerns in data computational analysis demand attention. Therefore, the research on machine learning based on homomorphic encryption is also constantly developing. Since then, many homomorphic encryption algorithms have appeared. At present, according to the types and quantities of operations allowed on encrypted data, homomorphic encryption algorithms can be divided into partial homomorphic encryption, somewhat homomorphic encryption, and full homomorphic encryption.

3.2.1. Partial Homomorphic Encryption (PHE)

PHE can only perform certain types of operations on ciphertext, such as addition, multiplication, or both, but only a limited number of operations are allowed. It mainly includes multiplication homomorphic encryption represented by the RSA (Rivest-Shamir-Adleman) algorithm and ElGamal algorithm, addition homomorphic encryption represented by the Paillier algorithm, and finite-degree homomorphic encryption represented by Boneh-Goh-Nissim scheme [4, 5]. RSA homomorphic encryption is one of the earliest homomorphic encryption algorithms proposed and widely studied. It uses the multiplication homomorphism of the RSA public key cryptosystem to perform multiplication operations on the ciphertext. However, the efficiency of RSA homomorphic encryption is relatively low, limiting its use in practical applications. Paillier homomorphic encryption algorithm is based on discrete logarithm problem and has high computational efficiency. It supports addition and multiplication on ciphertext and can solve the efficiency problem of RSA homomorphic encryption.

At present, PHE (Partial Homomorphic Encryption) algorithms are mainly used in the industry because of the constraints of performance and other factors. Paillier homomorphic encryption algorithm is widely used in the fields of security computing, privacy preservation and data sharing. PHE's (Partial Homomorphic Encryption) research focuses on its safety and computational efficiency.

3.2.2. Somewhat Homomorphic Encryption (SHE)

SWHE refers to homomorphic addition and homomorphic multiplication that can support a finite number of times, and homomorphic properties of cryptosystems are limited to addition or multiplication operations. Such as BGN05 scheme [6] it is constructed based on the difficult problem of bilinear mapping and can support not only any multiple homomorphic addition but also a homomorphic multiplication without increasing the length of the ciphertext.

3.2.3. Full Homomorphic Encryption (FHE)

A full homomorphic encryption algorithm can do infinite addition homomorphic and multiplicative homomorphic operations without decryption. It mainly includes the first-generation scheme represented by Gentry scheme, the second-generation scheme represented by BGV (Brakerski-Gentry-Vaikuntanathan) scheme and BFV (Brakerski-Fan-Vercauteren) scheme, the third-generation scheme represented by GSW (Gentry-Sahai-Waters) scheme, and the CKKS (Cheon-Kim-Kim-Song) scheme, which supports the approximate calculation of floating-point numbers and so on. FHE's research focuses on improving computing efficiency and reducing computing overhead.

3.3. The Development Stage of Homomorphic Encryption

The goal of homomorphic encryption algorithm, a significant area of study in cryptography, is to process data in its encrypted form while maintaining its confidentiality upon extraction. Gentry [3] proposed a fully homomorphic encryption algorithm that allows arbitrary computational operations to be performed on ciphertext [3]. That is, any operation can be performed on the plaintext of encrypted data without decryption. Over a decade of research has led to a rough division of the total homomorphic encryption algorithm into three stages. The three stages of FHE are shown in Table 2.

Table 2. The three stages of fully homomorphic encryption (FHE).

Generation	Feature	Scheme	Limitation
The first generation	● Based on ideal lattice construction ● Somewhat homomorphic encryption scheme ● To control the noise growth by bootstrapping technology	It is just the ideal Scheme	● Large key size ● High computational complexity ● Low efficiency ● Lack of practical application
The second generation	● Based on LWE (Learning with errors). ● Partial homomorphic encryption scheme ● To solve the problem of dimension expansion by key switching technology ● To control the noise by Modulus Switching technology ● Get rid of reliance on bootstrap technology ● Meets most applications	BGV(2011) LTV (Linder-Vaikuntanathan)(2012) BFV (Brakerski-Fan-Vercauteren) (2012) BLLN (Bos, Lauter, Loftus, and Naehrig) (2013)	● Public key size grows when using key exchange technology
The third generation	● Based on GSW (Gentry-Sahai-waters) ● The ciphertext is in matrix form ● It does not need key exchange technology and mode exchange technology ● It is no longer necessary to introduce the calculation key in the process of homomorphic calculation ● Use simpler algebraic operations	FHEW (Fast fully homomorphic encryption over the torus) (2014) TFHE (Torus fully homomorphic encryption) (2016)	● High computational cost ● Low execution efficiency

3.4. The Limitations of Homomorphic Encryption

The key to homomorphic encryption is that homomorphic encryption is its ability to perform computational operations on ciphertext while maintaining data confidentiality during the result extraction phase. This means that during the calculation process, no one can gain access to the original data, and only authorized users with the corresponding private key can decrypt and obtain the results. It protects the privacy of the data while also allowing users to perform calculations and actions without exposing the data itself. It is suitable for privacy preservation in big data scenarios.

The implementation of homomorphic encryption usually relies on mathematically complex algorithms and cryptographic principles, such as RSA homomorphic encryption, Paillier homomorphic encryption, and so on. These algorithms leverage challenging issues like discrete logarithm problems and large number decomposition to safeguard data confidentiality and enable encrypted computation operations. However, homomorphic encryption usually requires higher computing resources and longer encryption time, and low performance has always hindered the application of homomorphic encryption in big data environments.

At present, homomorphic encryption schemes still have many operational limitations [7-11].

3.4.1. Finiteness of Operation

Homomorphic encryption requires a fixed depth of multiplication, resulting in finiteness of addition and multiplication operations. Only integer data is supported. At present, homomorphic encryption cannot perform maximum, minimum, comparison, and exponential operations.

3.4.2. The Calculation Cost is Large

Homomorphic encryption's computational complexity is typically higher than that of traditional encryption algorithms, so it requires more computational resources and time.

3.4.3. Large Encryption Volume

Homomorphic encrypted ciphertext is usually longer than plaintext, which increases the cost of data storage and transmission.

3.4.4. Unable to Handle Large-Scale Data

Due to the high computational overhead, homomorphic encryption is usually unable to handle large-scale data. This means that it is only suitable for specific application scenarios, such as secure computing and privacy preservation of small-scale data.

3.4.5. Limited Security

Homomorphic encryption needs to be calculated under the premise of ensuring security, which may be limited for some specific operations. For example, in complete homomorphic encryption, if the wrong key or parameter is used, the results of the calculation may be leaked.

3.4.6. Relatively New Technology

Homomorphic encryption is a relatively new encryption technology, and its security and reliability need to be further verified and improved.

4. RELATED WORKS OF HORMOMORPHIC ENCRPTION

Homomorphic encryption, as an "ideal" scheme to achieve cloud computing security, has the outstanding feature that it can effectively compute the plaintext corresponding to the encrypted data without decrypting the encrypted user data. Due to the huge computation cost and space consumption inherent in homomorphic encryption, privacy-preserving decision tree classification algorithm is faced with the defects of low computational efficiency and large space consumption. In theory, the fully homomorphic encryption scheme can carry out infinite addition and multiplication operations, so that it can carry out arbitrary operations.

In order to make the continuous authentication system have the characteristics of high precision and privacy preservation, machine learning algorithm is combined with privacy preservation scheme, and homomorphic encryption scheme is combined with logistic regression, so that the system has the characteristics of privacy preservation and high precision, but the system takes a long time to run. Full homomorphic encryption is the highest level of homomorphic encryption technology, but its design and implementation are very complicated, and the computational efficiency is low. With the improvement of homomorphic encryption efficiency, there are many research achievements based on homomorphic encryption. In recommendation systems, national encryption will be an increasingly promising way to protect user privacy. Most of the research on using homomorphic encryption to train machine learning models and fully realize secure outsourcing computing uses the logistic regression algorithm.

Cheon, et al. [7] proposed the integrated gradient descent (GD) method of logistic regression, which reduced the expected number of GD iterations. Since the horizontal parameters of HE increase linearly with the number of iterations, the integration method gets a lot of results, which reduces the running time of the whole learning process in the encrypted state and the storage of encrypted data. Since the polynomial approximation of sigmoid function and the approximate calculation of homomorphic encryption for arithmetic of approximate numbers have small errors in each iteration, machine learning technology is selected as logistic regression, and HE scheme is selected as HEAAN (Homomorphic Encryption for Arithmetic of Approximate Numbers). However, the integration method is a general method that is applicable not only to the logistic loss function but also to any strongly convex loss function over a compact domain and any other HE schemes. This scheme achieved good performance in training small logistic regression models, but their solution only allowed the computation of a very small number of features.

Wei-jing, et al. [8] proposed a smart grid data aggregation scheme based on Homomorphic Encryption: improved group signature, Paillier encryption system, and ElGamal signature algorithm. This scheme not only anonymizes the real identity of users, provide fine granularity privacy preserving of electrical data, but also track the real identity of malicious signers. This scheme can greatly protect users' privacy information in smart power grids. It effectively solves the problem that smart electricity meters and other network devices leak users' privacy when collecting, processing, and transmitting a large amount of data.

Chandrakar and Hulipalled [9] proposed the use of pseudo-anonymity and homomorphic encryption to encrypt privacy, using Hadoop to realize homomorphic encryption. Since homomorphic encryption allows computation in encrypted data, data is split among multiple nodes in Hadoop cluster to perform parallel algorithms, which provides greater privacy and performance than previous methods. It also supports data mining in an encrypted form, ensuring that the cloud never sees the raw data during mining. Safer than existing technology. It outperforms prior art due to its implementation in the Map Reduce framework and its short running time.

Cortés-Mendoza, et al. [12] proposed three homomorphic cryptographic logistic regression gradient descent algorithms based on residual systems. These algorithms apply ciphertext to train, test, and execute predictions. Consequently, the algorithms allow for secure deployment in untrusted environments. The complicated tasks of managing and analyzing data are reduced in a cloud computing environment. The proposed algorithms are compared against four classical non-homomorphic logistic regression algorithms, a homomorphic algorithm based on the Residue Number System (RNS) and batch gradient descent, and two state-of-the-art homomorphic algorithms. The homomorphic algorithm working on encrypted data achieved nearly similar accuracy as the non-homomorphic, with resulting improvements, especially during the training process and classifying elicited data. This shows the practicality of training and classifying (in a logistic regression scenario) on encrypted models. However, further investigations of the efficiency and conciseness of the algorithms will be important so that polynomial approximation lengths and data set variability can be analyzed, including levels [10].

Homomorphic encryption has gained popularity with the rise of the internet and the cloud computing, as well as increasing demands for secure applications such as ciphertext search, electronic voting, and multi-party computing. Its advantages in computational complexity, communication complexity, and security have attracted growing research interest in theoretical and practical applications. For instance, homomorphic encryption can address privacy concerns in cloud computing environments by encrypting sensitive user data before analysis, such as medical and financial records. Additionally, it enhances the security of interactions between untrusted parties on blockchain systems [11].

With the improvement of homomorphic encryption efficiency, research results and applications based on homomorphic encryption have wide and important applications in ciphertext data computing under distributed computing environments, such as e-commerce, government data management, artificial intelligence, financial services, cloud computing, healthcare, etc. Homomorphic encryption technology can help e-commerce platforms protect user privacy and improve data security. In the field of government data management, homomorphic encryption technology can help government agencies protect the privacy of citizens' data and improve the efficiency of data processing and analysis. Homomorphic encryption can help healthcare organizations share patient medical data while protecting patient privacy. The use of homomorphic encryption in cloud computing can solve the problem that cloud service providers cannot guarantee the privacy of data [13]. Homomorphic encryption technology can realize the safe calculation and processing of data, while protecting the privacy of data. Homomorphic encryption technology can help banks and financial institutions achieve secure data processing and analysis. Financial institutions can use homomorphic encryption technology to encrypt customer data for calculation and analysis, thereby protecting the privacy and security of customer data.

Tian, et al. [14] proposed a remote authentication privacy protection scheme based on user biometrics for identity hiding, which adopted DT-PKC (Double Trapdoor Public Key Cryptosystem) homomorphic encryption algorithm to protect user behavior data. The security model included biometric and user privacy. A secure Euclidean distance computing protocol is constructed to authenticate user identity. The experimental results show that using 1024-bit DT-PKC algorithm, it takes 20s to run the secure Euclidian distance calculation protocol with 400-dimensional feature vectors.

Wei-jing, et al. [8] introduced a smart grid data aggregation scheme that integrates El-Gamal signature algorithm, Paillier encryption system, and an enhanced group signature with homomorphic encryption. This approach effectively conceals the identities of users while simultaneously safeguarding electrical data with greater precision. Also, it has the capability to monitor the genuine identities of malicious actors, thereby improving the security of the smart grid. During the collection, processing, and transmission of data, this method mitigates the privacy risks associated with network devices, including smart meters.

Chandrakar and Hulipalled [15] proposed a privacy-preserving methodology that utilizes pseudonymous and homomorphic encryption that is integrated into the Hadoop framework. The schemes partitions the encrypted across multiple nodes in a Hadoop cluster for parallel processing, thereby improving performance and privacy. In order to guarantee that the raw data remains concealed from the cloud during processing, it supports encrypted data mining. In addition to providing superior performance in comparison to existing methods, this approach also minimizes downtime when integrated into the MapReduce framework.

Kumar, et al. [16] developed a privacy protection scheme for healthcare centers that is specifically designed for decentralized multi-hospital platforms. This scheme is based on homomorphic encryption and blockchain architecture. Blockchain ledger technology eliminates the need for a central server, decentralizing federating learning models and enabling hospitals to securely share encrypted federated models while protecting data privacy. By combining blockchain and federated learning, a novel paradigm for the secure exchange of medical image data across decentralized networks is being introduced.

Although homomorphic encryption algorithm is important in theory and has been applied in some specific scenarios, its computational complexity and efficiency are still challenges to be solved. Current research focuses on algorithm design, improvement, and optimization, as well as exploring feasibility and practicality in practical applications. With the development of cryptography and computer science, more efficient and powerful homomorphic encryption algorithms are likely to emerge in the future.

5. CONCLUSIONS

Homomorphic encryption is an ideal scheme for cloud computing security. Its outstanding feature is that it can effectively calculate the plaintext of encrypted data without decrypting encrypted user data. Because of the huge computing cost and space consumption inherent in homomorphic encryption, privacy preservation decision tree classification algorithm faces the defects of low computing efficiency and large space consumption. In theory, the total homomorphic encryption scheme can perform an infinite number of addition and multiplication operations, so that arbitrary operations can be performed. Homomorphic encryption is widely used in cloud computing, privacy preservation, data sharing, and other fields. Researchers are exploring how to apply homomorphic encryption to more scenarios and developing corresponding application systems and tools. Homomorphic encryption plays an important role in secure cloud computing, privacy preservation, and data sharing. It enables privacy preservation and data processing without exposing sensitive personal information. However, because homomorphic encryption algorithms are so complex, their computational efficiency is relatively low, and it is still an active research field. In short, homomorphic encryption is a field full of challenges and opportunities, and its research and application prospects are very broad.

Funding: This study received no specific financial support.
Institutional Review Board Statement: Not applicable.
Transparency: The authors state that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: Conceptualization, formal analysis, investigation, and writing-original draft, Q.C.; data curation, methodology, and supervision, S.A.; conceptualization, writing-review & editing & software, N.A.S.A. All authors have read and agreed to the published version of the manuscript.

REFERENCES

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169-180, 1978.

[2] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," *IEEE Access*, vol. 4, pp. 1821-1834, 2016. https://ieeexplore.ieee.org/document/7460114

[3] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, 2009, pp. 169-178. https://doi.org/10.1145/1536414.1536440

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985. https://doi.org/10.1109/tit.1985.1057074

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes in international conference on the theory and applications of cryptographic techniques." Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223-238. https://doi.org/10.1007/3-540-48910-X_16

[6] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *In Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2 (pp. 325-341). Springer Berlin Heidelberg*, 2005. https://doi.org/10.1007/978-3-540-30576-7_18

[7] J. H. Cheon, D. Kim, Y. Kim, and Y. Song, "Ensemble method for privacy-preserving logistic regression based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 46938-46948, 2018. https://doi.org/10.1109/access.2018.2866697

[8] Z. Wei-jing, Z. He-chun, Y. Shi-ying, and L. Tong, "A homomorphic encryption-based privacy preserving data aggregation scheme for smart grid," presented at the In 2019 15th International Conference on Computational Intelligence and Security (CIS), 2019. https://doi.org/10.1109/CIS.2019.00073

[9] I. Chandrakar and V. R. Hulipalled, "Techniques for preserving privacy in data mining for cloud storage: A survey," in *In Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2 (pp. 452-461). Springer Singapore*, 2021. https://doi.org/10.1007/978-981-15-6353-9_42

[10] Z. Brakerski, N. Döttling, S. Garg, and G. Malavolta, "Candidate iO from homomorphic encryption schemes," *Journal of Cryptology*, vol. 36, no. 3, p. 27, 2023. https://doi.org/10.1007/s00145-023-09471-5

[11] X. Yu, W. Zhao, Y. Huang, J. Ren, and D. Tang, "Privacy-preserving outsourced logistic regression on encrypted data from homomorphic encryption," *Security and Communication Networks*, vol. 2022, no. 1, p. 1321198, 2022. https://doi.org/10.1155/2022/1321198

[12] J. M. Cortés-Mendoza *et al.*, "LR-GD-RNS: Enhanced privacy-preserving logistic regression algorithms for secure deployment in untrusted environments," presented at the In 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid) (pp. 770-775). IEEE, 2021. https://doi.org/10.1109/CCGrid51090.2021.00093

[13] Z. Xia, Q. Yang, Z. Qiao, and F. Feng, "Quorum controlled homomorphic re-encryption for privacy preserving computations in the cloud," *Information Sciences*, vol. 621, pp. 58-73, 2023. https://doi.org/10.1016/j.ins.2022.11.084

[14] Y. Tian, Y. Li, X. Liu, R. H. Deng, and B. Sengupta, "Pribioauth: Privacy-preserving biometric-based remote user authentication," presented at the In 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. https://doi.org/10.1109/DESEC.2018.8625169

[15] I. Chandrakar and V. R. Hulipalled, "Privacy preserving big data mining using pseudonymization and homomorphic encryption," presented at the In 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021. https://doi.org/10.1109/GCAT52182.2021.9587765

[16] R. Kumar *et al.*, "Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images," *Computerized Medical Imaging and Graphics*, vol. 102, p. 102139, 2022. https://doi.org/10.1016/j.compmedimag.2022.102139

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.