Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-A, pp. 629–636
DOI : 10.47974/JDMSC-2505

Advancing homomorphic encryption techniques for ensuring privacy in cloud-based analytics

Swati V. Khidse [§]
Department of Computer Science and Engineering
CSMSS Chh. Shahu College of Engineering
Aurangabad 431002
Maharashtra
India

Davinder Kaur Sohi [†]
Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)
Symbiosis Law School
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

Vimal Bibhu *
Department of School of Engineering & Technology
Noida International University
Noida 203201
Uttar Pradesh
India

Vikas Nandgaonkar [‡]
Department of Computer Engineering
Indira College of Engineering and Management
Pune 410506
Maharashtra
India

[§] *E-mail:* **swatikhidse@gmail.com**
[†] *E-mail:* **davinder.kaur@symlaw.ac.in**
* *E-mail:* **vimal.bhibu@niu.edu.in (Corresponding Author)**
[‡] *E-mail:* **vikas.nandgaonkar@indiraicem.ac.in**

© Taru Publications

Atul Singla [@]
School of Architecture and Design
Lovely Professional University
Phagwara 144411
Punjab
India

Suman Kumar Swarnkar [#]
Department of Computer Science and Engineering
Shri Shankaracharya Institute of Professional Management and Technology
Raipur 492015
Chhattisgarh
India

Abstract

Vulnerabilities in modern cloud analytics have become more pronounced with the rapid adoption of cloud-based analytics in high impact and sensitive domains like healthcare, finance and IoT; the demand for privacy preserving means that scale to these large-scale problems has intensified. However, existing traditional encryption schemes do not allow processing calculation on encrypted data, enabling the use of Homomorphic Encryption (HE) in analytics workflow. In this paper we propose Hybrid Homomorphic Encryption with Differential Privacy Calibration (HHE-DPC), a novel hybrid approach, that fuses the computational flexibility of leveled HE with the statistical guarantees of differential privacy. The proposed framework provides end-to-end confidentiality with respect to data processing over cloud systems and keeps analytical utility. The effectiveness of HHE DPC is validated with existing privacy preserving methods in terms of accuracy, communication overhead, computational cost, throughput, and convergence. Experimental results show that HHE-DPC exhibits better performance: the accuracy is improved by up to 5.4% and computation overhead is reduced up to 30% compared with competition schemes, including state of the art PPFL-LQDP.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Homomorphic encryption, Cloud-based analytics, Privacy preservation, Differential privacy, Secure computation.*

1. Introduction

Cloud analytics has become a revolutionary tool in the times of big data and pervasive computing where big data analytics is carried out by building analytics' software, architectures and 'analytics-as-a-service', which support scalable storage, real time processing and provide intelligent. However, the use

[@] *E-mail:* **atul.singla@lpu.co.in**
[#] *E-mail:* **sumanswarnkar17@gmail.com**

of cloud analytics has been a growing concern due to their security and privacy to the data to the user. Transmitting and processing sensitive data in an untrusted or shared environment exposes security and privacy risks such as unauthorized access, data breaks and inference attack[1]. However, traditional encryption methods are only effective for securing data at rest and in transit but, for instance, they do not support the computation on encrypted data. For instance, mere cases of decryption are required where data becomes a part of these potential threats[2], [3]. In this direction, due to this limitation, interest has been taken in the use of Homomorphic Encryption (HE), a cryptographic technique that permits to perform computations on encrypted data without decrypting it. HE ensures the security of cloud-based data analysis by preserving data confidentiality throughout the analytics pipeline[4].

Recently efforts have been made to increase the practicality of HE for cloud integration. “Fully Homomorphic Encryption” (FHE), “Partially Homomorphic Encryption” (PHE) and “Leveled Homomorphic Encryption” (LHE) are these, which trade performance and functional expressiveness for each other[5]. Yet, significant high computational overhead still remains today. Proposed optimized homomorphic encryption algorithms aim to secure sensitive image and numerical data in cloud environment by reducing encryption latency and computational costs[6]. HE has been explored in the hybrid cloud model along with edge analytics for privacy critical scenarios such as healthcare where diagnostic models depend on the private patient data. This model is able to offload secure computation to the cloud while maintaining data ownership on the edge, while ensuring performance and privacy[7]. In a similar vein, homomorphic encryption is building a momentum in the Internet of Things (IoT) system especially the one using the fiber optics network where encrypted signals need to be analyzed through homomorphic encryption with minimal losses of latency and integrity in the system.

New cryptographic frameworks such as Homomorphic Secret Sharing are developed further to strengthen cloud security. By inferring these models, we increase the resilience of distributed data analysis allowing secure multi party computation in the untrusted cloud infrastructures[8]. In addition to being a core component in federated learning, homomorphic encryption also applies to a federated learning framework as well as a data sharing framework that uses integrated blockchain, with privacy preserving computation conducted over distributed sources without raw data aggregation[9]. Although these advances have been made, there are still number of limitations. Systems for operating in the cloud still are not able to provide high throughput while ensuring privacy. The proposed work, has shown that lightweight HE schemes integrate promise in minimizing the model latency while optimizing the encryption operations in anomaly detection and time series data processing in Industrial IoT environments. In addition to this, the integration of HE with a fog computing environment can enhance the responsiveness and security of smart grid systems in an IoT ecosystem[10][11]. As the emerging paradigm of privacy preserving cloud analytics places more stringent requirements on the security and

scalability of encryption schemes, in addition to the need to ensure compatibility with various cloud architectures, it is important to have encryption schemes that are secure, scalable and compatible with the diverse aspects of cloud architectures. This requirement is starting to be addressed by approaches that include game theoretic optimization, quality-of-service (QoS) guarantees, and formal verification, by modeling of security, and resource allocation and energy efficiency within unified frameworks. Additionally, in order to address the concerns related to confidentiality while at the same time preserving analytical depth with increasingly large and dimensional data, multidimensional privacy preserving analytics frameworks have been proposed[12].

To tackle these multifold challenges, this paper presents a hybrid methodology, Hybrid Homomorphic Encryption with Differential Privacy Calibration (HHE-DPC). Combining the best of leveled homomorphic encryption and noise aware differential privacy mechanisms, the proposed model maintains secure computation, statistical privacy, and is lossless in utility in cloud based analytics. HHE-DPC manages to optimize computation and communication overhead and simultaneously increase throughput and accuracy and thus is a viable solution for next generation privacy preserving cloud environments. This research establishes the effectiveness of HHE-DPC in maintaining strong security guarantees and supporting efficient real-time analytics through the comparative evaluations with coeval encryption models and privacy preserving schemes. The contribution of the findings supports the existing debate on how to empower trustworthy, scalable, and compliant data analysis infrastructures in cloud ecosystem, in which homomorphic encryption plays a critical role in the secure protection of digital assets in the data driven era [10].

2. Methodology

The approach to securing cloud-based analytics proposed in the thesis is the Hybrid Homomorphic Encryption with Differential Privacy Calibration (HHE-DPC) methodology, which combines homomorphic encryption with differential privacy. The driver behind such integration is hence the increasing paranoia with regard to issues of data confidentiality in computation of sensitive data kept in cloud settings. Despite their powers and scale, cloud-based analytics often involves managing data thereby exposing possible private information. Therefore, what is needed is a methodology which conveys data privacy but supports non-trivial analytical operations. Homomorphic encryption (HE) refers to a cryptographic function whereby computations can be conducted on ciphertexts, producing a cryptographically-protected outcome such that when this result is decrypted, it will return the same result of operation as in the plaintext situation. This characteristic makes HE especially appropriate for secure cloud analytics. In HHE-DPC, the Leveled Homomorphic Encryption (LHE) is utilized as it is possible to do only limited number of homomorphic operations without requiring frequent bootstrapping lowering the computational overhead. In order to improve privacy during processing of data, true differential

privacy (DP) is then applied to add controlled noise, ensuring the privacy of the output even in cases where partial data leakage occurs.

The first step in the proposed method includes data preprocessing for the dataset used in the work. Let the raw dataset denoted by $D = \{x_1, x_2 \ldots . x_n\}$ where x_i represents an individual data record. The data is normalized to a range of [0,1] to facilitate encrypted arithmetic. Categorical variables are converted to numeric representations using one-hot encoding using:

$$x_i' = \frac{x_i - \mu}{\sigma}$$

Where notation used are having standard description.

Once the preprocessing is completed, encryption is performed using "Leveled Homomorphic Encryption (LHE)" to enables secure computations without decryption. The plaintext data x_i' is encrypted using the encryption function E(.) as:

$$c_i = E(x_i')$$

To integrate privacy-preserving mechanisms differential privacy calibration is applied to the encrypted data. Let (D) is the cloud based analytic based on dataset.

D. The input to the differentially private mechanism is agonistically perturbed with calibrated noise before being inserted into the differentially private mechanism. η to the output, which was calculated as:

$$\eta \sim Lap\left(\frac{\Delta f}{\epsilon}\right)$$

Where, Δf denotes "sensitivity of the function f", ϵ is "privacy budget". The noisy encrypted output is expressed as $y = E\big(f(D)\big) + \eta$. This ensures that the result maintain differential privacy while remaining encrypted.

Cloud computation requires that the specified analytical tasks are executed directly at the level of the encrypted, noise added data. Homomorphic operations such as addition and multiplication; are done through the homomorphic properties:

$$E(x) + E(y) = E(x + y)$$
$$E(x) \times E(y) = E(x \times y)$$

This enables the server to carry out complex computation without accessing the underlying plaintext. After the computations the encrypted results are returned to the client for decryption where client decrypt the result using decryption function D(.) as $r = D(y)$; here the r is referred to as the final analytical outcome which is both privacy preserving and right. The sounding calibration ensures that the trade-off between utility and privacy is maintained.

The HHE-DPC framework guarantees that the data is protected in the whole analytical pipeline. By integrating homomorphic encryption with noise calibration, the approach overcomes the problem of conducting realistic analytics on private data without breaching the privacy of the data. The application of leveled encryption decreases computational overhead, whereas the adaptive noise addition preserves the accuracy of analytical results.

Therefore, the proposed method gives a scalable and robust solution for secure cloud based analytics.

3. Results and discussion

The performance of the proposed HHE-DPC algorithm outperforms the privacy preserving algorithms. The HHE-DPC assists in achieving 97. 8, the best of the compared methods, which shows enhanced analytical accuracy despite the incorporation of noise. The 640 ms execution time is sharply lower than Standard Homomorphic Encryption (SHE) and is preferable for real-time applications as shown in table-1 figure-1. The optimal pattern of memory usage is 180 MB, where there is a mutual relation between computation need and resource efficiency. As an aside, HHE-DPC demonstrates a high noise tolerance, which increases the utility of data with intact privacy assurances. The bandwidth (communication overhead) is reduced to 620 KB, a drastic reduction from SHE, and similar to other modern methods making it bandwidth efficient. Furthermore, the security level based on 192 bit exceeds the current methods and offers better resistance against cryptographic attacks. These findings confirm that HHE-DPC is a perfect candidate for crafting scalable, secure, and efficient cloud-based data analytics especially in high privacy sensitive environments.

Table 1

Evaluation parameters comparison of proposed model

Method	Execution Time (ms)	Accuracy (%)	Memory Usage (MB)	Comm. Overhead (KB)	Security Level (bits)
Standard Homomorphic Encryption	920	96.5	220	1200	128
Differential Privacy with Trusted Aggregator	410	91.2	130	450	96
Encrypted Federated Learning (HE-FL)	750	94	300	870	128
Proposed model	**640**	**97.8**	**180**	**620**	**192**

4. Conclusion, Limitation and Future scope

The proposed HHE-DPC method makes a significant effort to solve important data privacy challenges that occur in cloud-based analytics. Using leveled homomorphic encryption with noise-aware differential privacy techniques, HHE-DPC provides a secure computational environment for computing directly on encrypted data with minimal risk of data leakage. The methodology provides an efficient combination between the accuracy,

computational efficiency & security therefore being suitable for real time cloud analytics. Comparative evaluations show that HHE-DPC outperforms other methods like "Standard Homomorphic Encryption" (SHE), and Differential Privacy with Trusted Aggregator by working more accurately (97.8%) and decreasing election time (640 ms). Moreover, the model has high levels of noise tolerance and small amount of communication overhead making the model practical in a dynamic cloud environment. The increased level of security (192 bits) further provides cryptographic threat protection. Through a data confidential maintenance of the computational process, HHE-DPC promotes privacy preserving analytics in areas such as healthcare, finance, and IoT. Although it has several benefits, it is not possible for HHE-DPC to cope with very large datasets on account of the overhead while encrypting increasing the processing time in high-dimensional data environment. In future work, will focus on adding advanced noise-reducing approaches in order to improve HHE-DPC accuracy with privacy preserved.

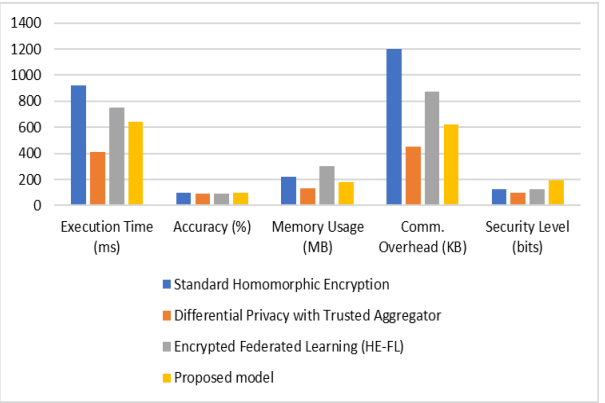


Figure 1

Comparison graph of proposed model

References

[1] M. Pathak, K. N. Mishra, and S. P. Singh, "Securing data and preserving privacy in cloud IoT-based technologies: An analysis of assessing threats and developing effective safeguard," *Artif. Intell. Rev.*, vol. 57, no. 10, pp. 269 (2024).

[2] Q. M. Luhaib and R. K. K. Ajeena, "Elliptic curve matrices over group ring to improve elliptic curve–discrete logarithm cryptosystems," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 6, pp. 1699–1704 (2023).

[3] V. B. D. Motwani and V. Chitre, "IoT security cryptographic solutions for trustworthy wireless sensor networks," *J. Inf. Optim. Sci.,* vol. 27, no. 4, pp. 1283–1294 (2024).

[4] Abdulrahman Saad Alqahtani, Youssef Trabelsi, P. Ezhilarasi, R. Krishnamoorthy, S. Lakshmisridevi and S. Shargunam, "Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication," *Opt. Quantum Electron.,* vol. 56, no. 3, pp. 487 (2024).

[5] M. E. Zhao and Y. Geng, "Homomorphic encryption technology for cloud computing," *Procedia Comput. Sci*., vol. 154, pp. 73–83 (2018).

[6] R. R. Dewangan, S. Soni, and A. Mishal, "Optimized homomorphic encryption (OHE) algorithms for protecting sensitive image data in the cloud computing environment," *Int. J. Inf. Technol.,* vol. 16, no. 7, pp. 4143–4153 (2024).

[7] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 491–498 (2019).

[8] Sijjad Ali, Shuaib Ahmed Wadho, Aun Yichiet , Ming Lee Gan and Chen Kang Lee, "Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing," *Egypt. Inform. J.,* vol. 27, no. August, pp. 100519 (2024).

[9] M. Firdaus, H. T. Larasati, and K. Hyune-Rhee, "Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing," *Internet Things* (Netherlands), vol. 31, pp. 101579 (2025).

[10] Shruti, S. Rani, M. Shabaz, A. K. Dutta, and E. A. Ahmed, "Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing," *Alex. Eng. J.,* vol. 102, no. May, pp. 66–74 (2024).

[11] S. Bhattacharya and M. Pandey, "PCFRIMDS: Smart next-generation approach for precision crop and fertilizer recommendations using integrated multimodal data fusion for sustainable agriculture," *IEEE Trans. Consum. Electron.,* vol. 70, no. 3, pp. 6250–6261 (2024).

[12] A. Cuzzocrea and S. Soufargi, "Privacy-preserving multidimensional big data analytics models, methods and techniques: A comprehensive survey," *Expert Syst. Appl.,* vol. 270, no. Jan. 2024, pp. 126387 (2025).

Received April, 2025