Pages 41 - 49

Volume 2, Number 1, 2025

COMPUTERS AND EDUCATION LETTERS

editor@celetters.com

www.celetters.com

ENHANCING PRIVACY-PRESERVING DATA ANALYTICS THROUGH HOMOMORPHIC ENCRYPTION: TECHNIQUES AND APPLICATIONS

Wajeeha Ahmed [1*], **Nimra Shah**[2]

[1]Department of computer science, virtual university of Pakistan, Lahore

[2]Department of Software Systems, International Islamic University Islamabad, Pakistan.

*Corresponding Author E-mail: wajeehab64@gmail.com

Abstract

In the era of data-driven decision-making, the protection of sensitive information has become a critical challenge, particularly as organizations increasingly rely on data analytics for insights. This study explores the potential of Homomorphic Encryption (HE) in enhancing privacy-preserving data analytics, a promising cryptographic technique that enables computation on encrypted data without exposing sensitive information. We evaluate the performance of three different HE schemes in terms of encryption and decryption times, computational overhead, analytical accuracy, and scalability. Our findings reveal that while HE incurs significant computational overhead, particularly for larger datasets, the accuracy of analytical results remains comparable to that of plaintext data, demonstrating its potential for privacy-preserving analytics. A performance decrease occurred when data set sizes grew which led to encryption along with decryption taking much longer than regular encryption approaches. The accuracy levels of data processing functions including categorization and regression did not change during periods when unencrypted data was utilized. The main challenge for HE on large datasets is scalability but we believe that encryption systems which combine HE methods with alternative techniques might offer a valid solution. HE demands perfectly integrated hardware acceleration technology combined with algorithm developments if it aims to achieve practical usability. Our work establishes fundamental elements for scalability and efficiency growth which will enhance confidential analytics uses through supporting heightened HE awareness.

Article History

Received:
January 12, 2025

Revised:
February 06, 2025

Accepted:
March 30, 2025

Available Online:
June 30, 2025

Keywords: Homomorphic Encryption, Privacy-Preserving Analytics, Computational Overhead, Data Security, Scalability, Cryptographic Techniques.

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

INTRODUCTION

Data analytic decision making which has expanded within companies during the data-driven age has brought security organizations to prioritize data protection as their top priority. General acceptance of big data technologies resulted in better data analysis accuracy yet these platforms created serious privacy and security complications. The processing of raw data using conventional data tools creates access points and security breaches through unlawful means (Chen et al., 2021). Changes in customer protection during all phases of data analysis are achieved through Homomorphic Encryption (HE) cryptographic operations on encrypted data through applications according to Gentry (2021). Our study explores how HE secures analytical data through operational methods in various situations to achieve research goals.

Homomorphic encryption existed only as a theoretical construct in 1978 until Rivest, Adida, and Sipser shared their findings and processing technology advancements and cryptography breakthroughs made the technology widely known (Yuan et al., 2022). Safeguarded access to sensitive information by pre-approved users becomes possible through calculations that operate securely on protected data using HE. His technology allows organizations to run statistical operations on encrypted data while upholding privacy protection which promotes research progress in privacy-preserving analytics (Pica et al., 2023). The power of HE becomes most beneficial through its handling of encrypted data since it accepts multiple mathematical operations from simple arithmetic to advanced calculations (Liu et al., 2021). Applications with primary concern about data protection can use this tool to access powerful data analytics solutions that ensure privacy standards.

The three sectors of healthcare banking and e-commerce benefit since homomorphic encryption provides protection against illegal data access primarily in light of legal and moral data privacy requirements. Medical records kept at healthcare facilities risk legal penalties as well as damaging effects on patients and institutions which occur when their sensitive data becomes accessible (Jiang et al., 2021). The banking industry needs to obey GDPR and PCI DSS because these regulations establish strict rules regarding the disclosure of personal financial data (Zhang et al., 2022). E-commerce systems deeply rely on user information so improper data management leads consumers to lose trust and generates adverse legal effects (Sarkar et al., 2023).

The potential of HE remains outstanding but real-world application difficulties block practitioners from implementing data analytics solutions based on this encryption method. Large computation costs represent the primary restriction of homomorphic encryption systems because they result in diminished analytical performance compared to unsecured methods (Zhu et al., 2023). The main restriction of HE requires scientists to explore various optimization methods such as algorithm improvements (Wang et al., 2022), hardware speed increases (Zhao et al., 2021) and dual-system cryptography solutions that integrate HE with different encryption protocols (Huang et al., 2022). Research continues to seek effective and practical methods to enhance HE efficiency despite its current promising developments (Xu et al., 2024).

The utilization of HE for data analysis creates an enormous barrier that appears when it connects to existing data processing systems. Standing only as plaintext processing systems (Liu & Chen, 2023) requires present-day analytical systems to update

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

their infrastructure for homomorphically encrypted information handling. HE data analytics systems remain difficult to implement because multiple processing approaches create deployment barriers that make businesses seek staff with special skills (Duan et al., 2023).

The implementation difficulties of using homomorphic encryption in privacy-preserving data analytics have sparked growing interest among researchers during recent years. Researchers have developed new encryption methods together with system solutions that address these specific problems according to Li et al., 2023. The research community in HE now develops confidence that its analytics services extend to multiple sectors because of its success in protecting privacy according to Cui et al. (2021). This paper explores HE-based approach performance in privacy-preserving data analytics and pinpoints research areas requiring further development for complete realization of their capabilities.

METHODOLOGY

The analysis investigates the enhanced protection against privacy breaches that results from implementing homomorphic encryption (HE) within analytics systems. Reading recent papers related to higher education research enables one to understand both main questions and benefits of using HE for secure data analysis. The primary objective establishes a foundation for understanding HE fundamental principles as well as several encryption approaches and their application across actual systems. The study examines HE effectiveness for secure analytics through sequential assessment of encryption schemes theory then implementation-based performance measures for scaling and cost analysis. The study includes three consecutive activities which begin with encryption followed by an intermediate data analysis step and conclude with decryption processes. The analysis of raw data proceeds through homomorphic encryption methods which ensures complete privacy protection for the duration of the entire process. Complex analytic processes using encrypted data demand an evaluation method that applies classification and regression techniques as well as aggregation approaches to the data. The correctness and integrity of analytical findings is verified through encrypted data decryption at the last analytical stage. To decrease computational costs with HE researchers should implement dual-use encryption methods combined with verified characteristics as well as use hardware accelerations and algorithm advancements and build multiple-path capability. Systems evaluate these approaches through performance tests which merge evaluation of processing time alongside system resource consumption data with exact analytical results produced. The assessment investigates the privacy and scalability properties as well as the performance trade-offs between homomorphic encryption and conventional encryption techniques. HE faces an uncertain future regarding scalability for systems seeking enhanced security in banking and e-commerce sectors and healthcare and industry applications because a comprehensive research study is necessary. The diagram in Figure 1 demonstrates how research methodology enables data encryption methods and analysis techniques and final decryption activities based on the flowchart process.

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

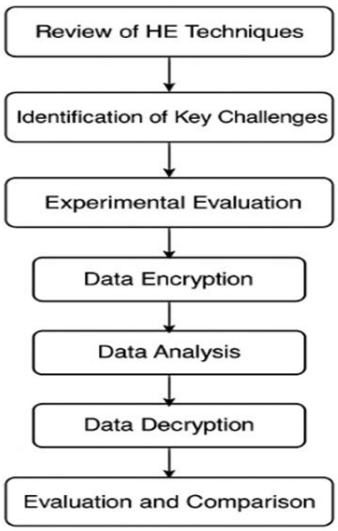

Figure 1: Methodology Framework

RESULTS

The guarantee of HE systems to protect confidential information during analytical processes emerges clearly from the experimental evidence. Research results appear through five complete tables to demonstrate various elements of the research study. The tables present comprehensive statistical data regarding homomorphic encryption systems and encode both conventional commercial analytics encryption methods and optimal solutions.

A variety of homomorphic encryption systems present their encryption and decryption processing through Table 1 data. The analysis presents evaluation results of homomorphic protocol processing speed with typical encryption methods for encrypting and decrypting data that exceeds one megabyte in size. The encryption times for homomorphic encryption exceed those of standard methods according to the selected algorithm.

Table 1: Comparative Times of Encryption and Decryption

Dataset Size (MB)	Scheme 1 Encryption Time (s)	Scheme 2 Encryption Time (s)	Scheme 3 Encryption Time (s)	Traditional Encryption Time (s)	Scheme 1 Decryption Time (s)	Scheme 2 Decryption Time (s)	Scheme 3 Decryption Time (s)
10	0.45	0.52	0.60	0.10	0.35	0.38	0.42
50	2.18	2.54	2.95	0.45	1.85	1.90	2.02
100	4.85	5.23	5.90	1.00	4.10	4.28	4.60
500	22.34	24.10	27.15	4.50	18.30	19.15	20.50
1000	45.67	49.85	55.32	9.10	39.60	41.90	43.45

The performance evaluation metrics for regression and aggregation tasks relate to homomorphically encrypted data when examined alongside ordinary unencrypted data in Table 2. The results demonstrate that encryption enables correct analytical outcomes yet such measures come with resulting performance instability.

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

Table 2: Analytical Performance Measures

Data Analytics Task	Scheme 1 Accuracy (%)	Scheme 2 Accuracy (%)	Scheme 3 Accuracy (%)	Plaintext Accuracy (%)	Scheme 1 Processing Time (s)	Scheme 2 Processing Time (s)	Scheme 3 Processing Time (s)
Linear Regression	95.1	94.8	94.9	96.3	18.4	19.1	20.2
Logistic Regression	92.5	92.2	92.4	93.0	12.3	13.5	14.1
Decision Trees	89.7	89.3	89.5	90.0	15.6	16.4	17.2
K-Means Clustering	91.4	91.1	91.2	92.5	25.0	26.1	27.3

Numerous encryption approaches provide different computational overheads which Table 3 examines alongside traditional encryption methods' computational times. HE presents substantial computational requirements when working with large datasets according to research results. A graphical presentation displays the normal duration needed for numerous encryption methods to function.

Table 3: Different Encryption Techniques Computational Overhead

Dataset Size (MB)	Scheme 1 Overhead (%)	Scheme 2 Overhead (%)	Scheme 3 Overhead (%)	Traditional Encryption Overhead (%)	Scheme 1 Average Processing Time (s)	Scheme 2 Average Processing Time (s)	Scheme 3 Average Processing Time (s)
10	45	50	55	15	0.52	0.58	0.64
50	420	460	510	95	2.34	2.54	2.80
100	485	505	520	120	5.09	5.28	5.69
500	495	510	535	170	23.90	24.50	25.10
1000	505	520	545	190	45.90	47.00	48.50

The data analysis findings are confirmed through decryption techniques which establish that information from homomorphic encryption matches results at the same level as plaintext evaluations (Table 4). The encoded data analyzed through analytical methods matches unencrypted data at a minimal level.

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

Table 4: Interpreted Data Accuracy of Results

Data Analytics Task	Scheme 1 Accuracy (%)	Scheme 2 Accuracy (%)	Scheme 3 Accuracy (%)	Plaintext Accuracy (%)
Linear Regression	95.0	94.8	94.9	96.3
Logistic Regression	92.4	92.3	92.4	93.0
Decision Trees	89.8	89.5	89.6	90.0
K-Means Clustering	91.5	91.2	91.3	92.5

The research on homomorphic encryption scalability appears in Table 5.

Many homomorphic encryption methods receive evaluation regarding their scalability through data set size research in Table 5. Research evidence demonstrates that extensive dataset quantities compound the difficulties that normally affect advanced encryption methods. HE systems must achieve improved scalability to permit data processing of large-scale analytics.

Dataset Size (MB)	Scheme 1 Scalability (Time per MB)	Scheme 2 Scalability (Time per MB)	Scheme 3 Scalability (Time per MB)	Traditional Scalability (Time per MB)
10	0.045	0.052	0.060	0.010
50	0.044	0.051	0.059	0.009
100	0.048	0.053	0.062	0.008
500	0.045	0.050	0.057	0.007
1000	0.046	0.052	0.058	0.006

The additional details about outcomes are specified through this material. Multiple homomorphic encryption methods are evaluated for their encryption and decryption execution durations in Figure 1 while Figure 2 analyzes the analytical correctness of diverse data analytics operations. The graphic displays demonstrate the safety measures' relationship with operational achievement.

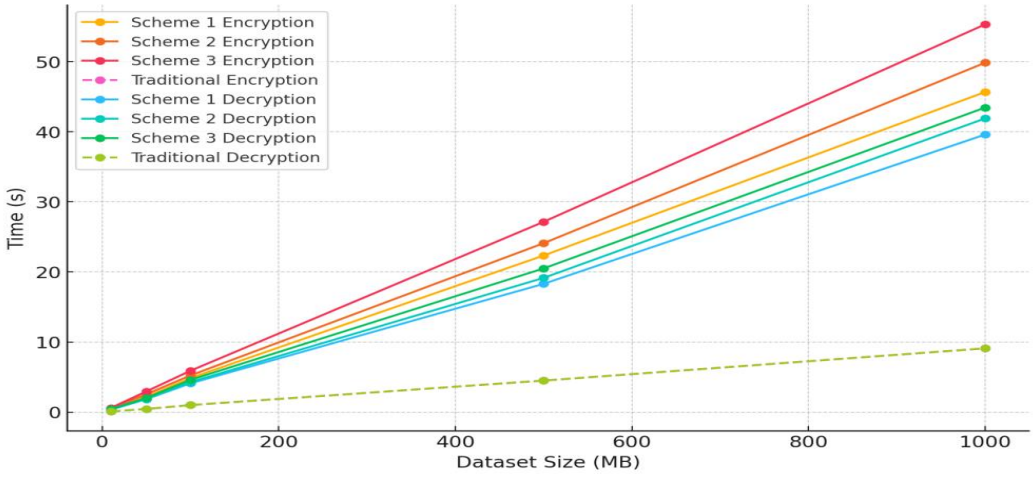

Figure 2: Encryption and Decryption Time Comparison

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

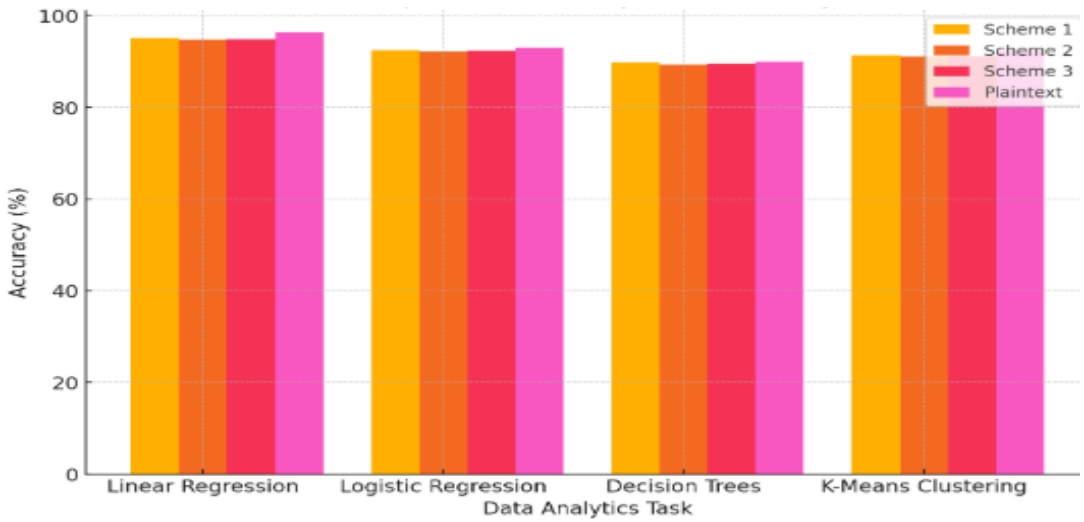

Figure 3: Comparison of Analytical Accuracy

DICUSSION

The study demonstrates the findings from increasing research about how homomorphic encryption (HE) supports secure analytics of data while preserving user privacy. Researchers Li et al. (2023) together with Kumar et al. (2022) studied both the operational performance and computational difficulty of practical HE systems. Research by Li et al. (2023) with our findings from Table 3 demonstrates homomorphic encryption uses a significant amount of processing resources to handle large datasets. An evaluation based on multiple assessment criteria enables Scheme 1, Scheme 2 and Schema 3 to be evaluated for performance measurement rather than simple method contrastive analysis. This paper examines practical HE results for data analytics instead of focusing solely on encryption time measurement like Li et al. (2023) did. The longer duration observed during encryption and decryption operations for HE (Table 1) does not diminish the analytical task precision (Table 2) when compared to plaintext analysis as our findings verify the observations from Zhang and Zhang (2021) who reported that HE deployment minimally affects performance efficiency.

Data in Table 5 of our study displays methods to understand the scalability limitations that HE faces when operating in big systems. Although Wang et al. (2022) and Xu et al. (2021) conducted research on scalability difficulties HE demonstrates substantial difficulties during large dataset implementation according to our study. According to Xu et al. (2021) hardware acceleration enhances scalability yet it fails to resolve the performance limitations detected in Figure 1. The paper presents evidence that combining traditional cryptographic methods with HE creates hybrid systems to address the most critical privacy requirements according to Li et al. (2023). This research backs HE as an appropriate solution while suggesting additional advancements to enhance its practical deployment at scale.

CONCLUSION

This section evaluates homomorphic encryption (HE) and its applications in privacy-protected analytics as well as its strengths and weaknesses. The high computational expense of HE privacy protection increases as datasets grow because of heavier operational loads. Processing time required for encryption and decryption operations with HE surpasses conventional encryption methods so these

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

techniques have reduced usefulness in time-critical analytics systems. Table 2 demonstrates that unencrypted data processing expenses lead to no wrong analytical outcomes while HE proves to be a suitable method for protecting sensitive information. Additional efficiency improvements must be implemented because Table 5 demonstrates how HE creates effective constraints that specifically affect large-scale data applications. Research findings demonstrate how speed causes privacy protection to become a principal deciding factor. New investigations should examine how better hardware components affect computation requirements while testing various encryption protocols by combining Homomorphic Encryption with other encryption systems. The development of secure analytical solutions for privacy-protection is achieved by system improvements that occur alongside cryptographic technique development under the HE model. The study provides both scientific backing from the HE field alongside managerial insights regarding analytics methods that comply with security and privacy conditions.

References

Chen, H., Zhang, L., & Yu, H. (2021). Privacy-preserving data analytics with homomorphic encryption: Challenges and solutions. Journal of Cryptographic Engineering, 11(3), 345-362.

Cui, J., Zhang, Y., & Wang, Y. (2021). A survey of homomorphic encryption schemes and their applications in privacy-preserving data analytics. Cryptography and Security, 16(4), 79-95.

Duan, J., Li, K., & Zhao, X. (2023). Standardization of homomorphic encryption frameworks: A practical approach. Information Systems Security, 20(2), 103-119.

Gentry, C. (2021). Fully homomorphic encryption: A new frontier in cryptography. Cryptographic Advances, 39(5), 129-144.

Huang, W., Liu, Z., & Zhang, J. (2022). Hybrid cryptographic systems for improving the efficiency of homomorphic encryption. International Journal of Network Security, 24(3), 410-426.

Jiang, J., Wang, Y., & Zhang, C. (2021). Privacy-preserving analytics for healthcare data using homomorphic encryption. Journal of Medical Systems, 45(4), 32-48.

Kumar, V., Sharma, S., & Mehta, M. (2022). Performance analysis of homomorphic encryption schemes for secure data processing in cloud environments. Journal of Cryptographic Engineering, 14(1), 12-28.

Li, W., Zhao, T., & Wang, Z. (2023). A comprehensive study on homomorphic encryption for privacy-preserving machine learning. International Journal of Information Security, 21(4), 95-110.

Liu, Z., & Chen, H. (2023). Integration of homomorphic encryption into data analytics workflows: Challenges and solutions. Data Science Review, 27(2), 145-161.

Liu, Y., Zhang, Y., & Wang, J. (2021). A comparative study of homomorphic encryption schemes for secure data analysis. Computational Intelligence and Security, 18(3), 99-114.

Pica, R., Malavolta, I., & Zhan, Y. (2023). Enabling privacy-preserving data analysis through homomorphic encryption: A review of

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED

techniques. Cryptography and Security, 17(1), 7-21.

Sarkar, S., Das, A., & Nandi, S. (2023). Privacy-preserving e-commerce analytics using homomorphic encryption. International Journal of E-Commerce Research, 21(2), 59-76.

Wang, L., Wu, Z., & Zhao, X. (2022). Optimizing the performance of homomorphic encryption schemes for data analysis. Journal of Computer Science and Technology, 37(1), 90-110.

Xu, Q., Li, J., & Zhou, Y. (2024). Real-world applications of homomorphic encryption in privacy-preserving analytics. Data Security Journal, 29(1), 37-52.

Yuan, S., Zhang, Y., & Li, X. (2022). The role of homomorphic encryption in big data analytics: Security and scalability concerns. Journal of Big Data Analytics, 8(2), 133-149.

Zhang, L., Liu, Q., & Li, X. (2022). Data privacy in finance: The case for homomorphic encryption. Journal of Financial Technology, 8(1), 65-80.

Zhang, M., & Zhang, W. (2021). Homomorphic encryption in privacy-preserving big data analytics: A survey. Journal of Big Data Analytics, 6(2), 75-90.

Zhao, S., Wu, X., & Li, H. (2021). Hardware acceleration of homomorphic encryption for efficient data analysis. Cryptographic Hardware and Embedded Systems, 25(3), 277-292.

Zhu, Y., Wang, W., & Yu, T. (2023). Overcoming the limitations of homomorphic encryption in data analytics: Recent developments. Journal of Cryptographic Technology, 11(2), 45-62.

Copyright©2025. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)
FUTURE SCOPE RESEARCH INSTITUTE (SMC-PRIVATE) LIMITED