Check for updates

RESEARCH ARTICLE

Applications of Homomorphic Encryption in Secure Computation

[version 1; peer review: 1 approved with reservations, 1 not approved]

Elissa Mollakuqe[1], Arber Parduzi[2], Shasivar Rexhepi[2], Vesna Dimitrova[3], Samir Jakupi[2], Rilind Muharremi[2], Mentor Hamiti[4], Jusuf Qarkaxhija[2]

[1]Kadir Has Universitesi, Istanbul, İstanbul, Turkey
[2]AAB College, Prishtina, Prishtina, Kosovo (Serbia and Montenegro)
[3]Saints Cyril and Methodius University in Skopje, Skopje, Skopje, North Macedonia
[4]South East European University, Tetovo, Tetovo, North Macedonia

v1 **First published:** 29 Jul 2024, **4**:158
https://doi.org/10.12688/openreseurope.18052.1
Latest published: 29 Jul 2024, **4**:158
https://doi.org/10.12688/openreseurope.18052.1

Abstract

Background

Homomorphic encryption (HE) represents a pivotal innovation in modern cryptography, offering a pathway to secure computation on encrypted data. This paper embarks on a comprehensive exploration of HE's applications, elucidating its transformative potential in bolstering data security and privacy across various domains.

Methods

The research employs a mixed-methods approach to evaluate HE technologies. Quantitatively, it develops realistic datasets simulating healthcare and financial data, assessing HE's performance in encrypted computations. Various encryption schemes are rigorously tested for efficiency and accuracy under different conditions. Qualitatively, insights from expert interviews and case studies of HE implementations provide additional context on practical challenges and strategic benefits.

Results

The simulations and analyses showcase the efficiency, scalability, and security of HE techniques in diverse scenarios. The empirical evidence validates the real-world applicability of HE, demonstrating its versatility and efficacy in secure computation outsourcing, privacy-

Open Peer Review

Approval Status ? ✗

	1	2
version 1 29 Jul 2024	? view	✗ view

1. **Yulliwas Ameur**, CEDRIC Lab, Conservatoire National des Arts et Métiers (Cnam), Paris, France
2. **Saja J. Mohammed**, University of Mosul, Mosul, Iraq

Any reports and responses or comments on the article can be found at the end of the article.

preserving data analysis, and secure multi-party computation.

Conclusions

This research paper highlights the transformative power of homomorphic encryption, advocating for its widespread adoption and integration. By bridging the gap between theoretical understanding and practical implementation, the paper contributes to advancing secure computation practices, addressing contemporary challenges in data security and privacy amidst evolving cybersecurity threats and the increasing ubiquity of sensitive data. In essence, this research serves as a beacon of insight into the future of data confidentiality and integrity, promoting HE as a crucial tool for revolutionizing the landscape of data security and privacy in an interconnected world.

Plain language summary
This research investigates homomorphic encryption (HE), a cutting-edge technology that allows computations to be performed on encrypted data without needing to decrypt it first. This capability is crucial for protecting sensitive information in fields like healthcare and finance, where data privacy is paramount. The study uses a mix of methods: it creates realistic datasets to test HE's performance in handling tasks like arithmetic and statistical analysis under various conditions. Additionally, insights from interviews with experts and real-world case studies shed light on practical challenges and benefits of HE. By combining these approaches, the research aims to provide a comprehensive evaluation of HE's effectiveness in enhancing data security and privacy, informing future developments in cryptographic techniques.

Keywords
Homomorphic, encryption, secure, computation and application.

This article is included in the Electrical, Electronic and Information Engineering gateway.

This article is included in the COST Actions gateway.

This article is included in the Fintech and AI in Finance collection.

Corresponding author: Elissa Mollakuqe (elissamollakuqe@gmail.com)

Author roles: Mollakuqe E: Conceptualization, Supervision, Visualization, Writing – Original Draft Preparation, Writing – Review & Editing; **Parduzi A**: Formal Analysis, Software; **Rexhepi S**: Software, Writing – Review & Editing; **Dimitrova V**: Methodology, Validation; **Jakupi S**: Conceptualization, Software; **Muharremi R**: Software; **Hamiti M**: Visualization, Writing – Review & Editing; **Qarkaxhija J**: Data Curation, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: This project has received funding from the European Union's Framework Programme for Research & Innovation as part of the COST Action [CA 19130 Fintech and AI in Finance], as supported by the COST Association (European Cooperation in Science and Technology).
The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Copyright: © 2024 Mollakuqe E *et al*. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Mollakuqe E, Parduzi A, Rexhepi S *et al.* **Applications of Homomorphic Encryption in Secure Computation [version 1; peer review: 1 approved with reservations, 1 not approved]** Open Research Europe 2024, **4**:158 https://doi.org/10.12688/openreseurope.18052.1

First published: 29 Jul 2024, **4**:158 https://doi.org/10.12688/openreseurope.18052.1

Introduction

Homomorphic encryption stands as a beacon of innovation within the domain of modern cryptographic techniques[1]. Its ability to enable secure computation on encrypted data opens up a realm of possibilities across diverse domains. In an era characterized by an exponential growth in digital platforms and the ubiquitous presence of sensitive data, the urgency for robust encryption methods has never been more pronounced. This research paper we begin this exploration to explore the numerous applications applications of homomorphic encryption, poised to catalyze a paradigm shift in secure computation and data privacy. As organizations and individuals alike grapple with the complexities of safeguarding their data in an increasingly interconnected world, homomorphic encryption emerges as a potent solution. Its promise lies in its capability to perform computations on encrypted data without the need for decryption, thereby preserving the confidentiality and integrity of sensitive information. This fundamental property paves the way for transformative applications across a spectrum of domains, from cloud computing to healthcare analytics and collaborative decision-making[2]. By venturing into the heart of homomorphic encryption, this paper aims to illuminate its transformative potential and chart a course towards enhanced data security and privacy. Through a comprehensive exploration of its applications, ranging from secure outsourcing of computations to privacy-preserving data analysis and secure multi-party computation, this research endeavors to showcase the versatility and efficacy of homomorphic encryption in addressing contemporary challenges. This paper seeks to bridge the gap between theoretical understanding and practical implementation by presenting experimental findings that validate the real-world applicability of homomorphic encryption. By providing concrete evidence of its efficacy and performance metrics, this research aims to instill confidence in the viability of homomorphic encryption as a cornerstone for secure computation. In essence, this research paper serves as a beacon of insight into the transformative power of homomorphic encryption. It is a call to action for researchers, practitioners, and policymakers to embrace this innovative cryptographic technique and harness its potential to revolutionize the landscape of data security and privacy. As we embark on this journey, let us not only explore the applications of homomorphic encryption but also lay the foundation for a future where data confidentiality and integrity are upheld without compromise. This research paper is motivated by the pressing need for robust encryption methods amidst escalating cybersecurity threats and the widespread presence of sensitive data. Traditional encryption techniques struggle when it comes to performing computations on encrypted data without decryption, posing challenges to secure computation and data privacy. Homomorphic encryption emerges as a groundbreaking solution, enabling secure computation on encrypted data while preserving confidentiality. This paper aims to explore its transformative potential in various domains, from secure outsourcing of computations to privacy-preserving data analysis and secure multi-party computation. The motivation for this exploration lies in homomorphic encryption's promise to address contemporary challenges in data security and privacy by allowing computations directly on encrypted data. By bridging theory and practice and presenting experimental findings, this paper seeks to inspire stakeholders to embrace homomorphic encryption as a cornerstone for enhancing data security and privacy. In essence, this research paper recognizes homomorphic encryption as a beacon of innovation with the potential to revolutionize data security and privacy. It aims to pave the way for a future where data confidentiality and integrity are maintained without compromise.

Fundamentals of homomorphic encryption and applications of homomorphic encryption

In this chapter, we delve into the rich landscape of literature surrounding homomorphic encryption, exploring its theoretical foundations, practical implementations, and applications across various domains[3]. The literature review serves as a critical foundation for understanding the evolution of homomorphic encryption and its implications for secure computation and data privacy[4]. The journey into homomorphic encryption begins with seminal works such as Craig Gentry's paper on "Fully Homomorphic Encryption over the Integers" (2009), where the concept of fully homomorphic encryption was introduced. Gentry's groundbreaking research laid the groundwork for subsequent advancements in the field, inspiring further exploration into the theoretical underpinnings of homomorphic encryption[5]. Building upon Gentry's work, researchers such as Zvika Brakerski and Vinod Vaikuntanathan proposed alternative constructions based on the learning with errors (LWE) problem, as evidenced in their paper "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler,Asymptotically-Faster,Attribute-Based" (2011). This paper contributed to the development of simpler and more efficient homomorphic encryption schemes, driving innovation in both theory and practice. Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi provided valuable insights into the practical aspects of homomorphic encryption in their survey paper "Homomorphic Encryption: Theory and Implementation" (2014). This comprehensive overview explored various implementation techniques, security considerations, and performance optimizations, bridging the gap between theoretical research and real-world applications[6]. Homomorphic encryption finds applications across a myriad of domains, from secure outsourcing of computations to privacy-preserving data analysis and collaborative decision-making[7]. Works such as Shai Halevi and Hugo Krawczyk's paper on "Cryptographic Methods for Secure Outsourcing of Computation" (2011) shed light on the practical protocols and applications of homomorphic encryption in securely delegating computation tasks to untrusted servers. In the realm of privacy-preserving data mining, Charu C. Aggarwal's book "Privacy-Preserving Data Mining: Models and Algorithms" (2008) explores the intersection of homomorphic encryption and data analysis, highlighting its role in enabling secure data mining while preserving privacy[8]. Advancements in secure multi-party computation (MPC) techniques, as discussed in the book "Secure Multi-Party Computation: Concepts and Applications" (2017), underscore the potential of homomorphic encryption in facilitating collaborative data analysis and decision-making

without compromising data privacy. The literature review reveals a vibrant ecosystem of research surrounding homomorphic encryption, with ongoing efforts aimed at advancing theoretical understanding, improving practical implementations, and exploring new applications[9]. As we navigate through the chapters of this research paper, we will draw upon insights gleaned from this comprehensive review to inform our exploration of homomorphic encryption's transformative potential in the realms of secure computation and data privacy. Homomorphic encryption stands apart as an encryption method that allows mathematical operations on data to be carried out on ciphertext, instead of the actual data itself[10]. It is operated on and then decrypted in order to obtain the desired result. The critical property of homomorphic encryption is that the same output should be obtained from decrypting the operated cipher text as from simply operating on the initial plain text[11]. With homomorphic encryption, the data can be encrypted (in a special way), computation can be done on the encrypted data, and the result is the encrypted answer. So, computing on the plaintext data will yield the same answer as computing on the encrypted data and decrypting the result.

One application of homomorphic encryption is to store your encrypted data in a public cloud and do computations on the encrypted data, without needing to trust the cloud not to leak your data[6]. Homomorphic encryption can be achieved as long as both operations such as (***and/multiply***) and (***xor/add***) can be performed with a circuit. There are schemes where it is possible to do one without the other[12]. RSA Encryption (without padding) can do multiplication homomorphically. Homomorphic encryption, a cornerstone of modern cryptography, comes in different flavors with distinct properties tailored to various use cases[13]. Two types of homomorphic encryption are: Fully homomorphic encryption (FHE) and Partially homomorphic encryption (PHE)[14]. FHE (see Table 1) allows for both addition and multiplication operations on encrypted data, offering the flexibility to perform arbitrary computations without decryption[4]. Its computational requirements are typically higher compared to partially homomorphic encryption schemes.

PHE (see Table 2) on the other hand, supports either addition or multiplication operations on encrypted data, but not both simultaneously[2]. While PHE may not offer the same level of versatility as FHE, it often requires less computational overhead and is suitable for scenarios where only specific types of computations need to be performed on encrypted data.

Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data, which when decrypted, will yield the same result as if the operations had been performed on the plaintext[3]. This characteristic makes it extremely valuable for securely processing sensitive data in untrusted environments, such as cloud computing.

Example of homomorphic encryption

Imagine you want to compute the sum of two numbers, but you want to ensure that the numbers remain confidential

Table 1. Fully Homomorphic Encryption.

Property	Description
Operates on	Allows both addition and multiplication operations on encrypted data.
Decryption	Supports arbitrary circuits, meaning any computation can be performed on encrypted data.
Security Level	Typically requires higher computational resources compared to partially homomorphic encryption schemes.
Applications	Suitable for scenarios where complex computations need to be performed on encrypted data, such as secure multi-party computation.

Table 2. Partially Homomorphic Encryption.

Property	Description
Operates on	Supports either addition or multiplication operations on encrypted data, but not both.
Decryption	Limited to specific operations, such as either addition or multiplication, depending on the encryption scheme.
Security Level	Generally requires less computational overhead compared to fully homomorphic encryption schemes.
Applications	Useful for applications where only specific types of computations need to be performed on encrypted data.

throughout the process. You can use homomorphic encryption to achieve this. Let's say the numbers are 5 and 3.

Encryption of Data:
First, each number is encrypted. Let's denote the encryption of a number ***\(x \)*** *as* ***\(E(x) \)****. So, we have* ***\(E(5) \)*** *and* ***\(E(3) \)****.*

Performing Operations on Encrypted Data
With homomorphic encryption, you can directly perform operations on the encrypted data. In this case, we want to perform an addition, so we calculate ***\(E(5) + E(3) \)****. Let's denote this operation as* ***\ (E (5) \+ E (3) \)****, where* ***\(\+ \)*** *represents the encrypted addition operation.*

Decryption of Result
Finally, the result of the encrypted operation is decrypted. This means decrypting ***\ (E (5) \+ E (3) \)*** *to get* ***5 + 3.***

In this example, the actual sum 8 is never exposed until the final decryption is performed, and all intermediate computations are done on encrypted data.

Privacy-preserving data analysis

Privacy-preserving data analysis represents a crucial domain where the application of homomorphic encryption offers significant advantages, particularly in sensitive sectors like healthcare analytics and financial forecasting[5]. Homomorphic encryption allows for data analysis to be conducted on encrypted data without compromising the privacy of individuals or organizations. In healthcare analytics, for instance, homomorphic encryption enables researchers and analysts to perform computations on encrypted patient data while preserving the confidentiality of sensitive health information. This capability facilitates collaborative research efforts and data sharing among healthcare institutions without the risk of exposing patient privacy[1]. Researchers can analyze encrypted patient records to identify trends, patterns, and correlations relevant to disease diagnosis, treatment efficacy, or epidemiological studies, all while ensuring that individual patient data remains confidential[15]. Similarly, in financial forecasting and analysis, homomorphic encryption can be employed to protect sensitive financial data while allowing for meaningful analysis[7]. Financial institutions can perform encrypted computations on customer transaction data, market trends, or investment portfolios without exposing sensitive information to unauthorized access. This enables banks, investment firms, and financial analysts to generate accurate forecasts, assess risk, and make informed decisions while safeguarding the privacy of their clients' financial information[8]. The advantages of preserving data privacy through homomorphic encryption are manifold. First and foremost, it ensures compliance with data protection regulations and privacy laws, such as HIPAA in healthcare or GDPR in finance, by minimizing the risk of data breaches or unauthorized access[9]. Homomorphic encryption promotes trust and transparency among stakeholders, as individuals and organizations can confidently share data for collaborative analysis without fear of privacy violations[16]. Preserving data privacy fosters innovation by encouraging data sharing and collaboration in research and analytics, ultimately leading to advancements in healthcare outcomes, financial services, and other domains[17]. The application of homomorphic encryption in privacy-preserving data analysis offers a powerful solution for conducting meaningful analysis while upholding data privacy and confidentiality[18]. By leveraging homomorphic encryption techniques, organizations can unlock the full potential of their data assets for research, analytics, and decision-making, all while ensuring the protection of sensitive information and maintaining compliance with privacy regulations.

Secure multi-party computation

Secure multi-party computation (SMPC) is a cryptographic technique that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private[19]. Homomorphic encryption plays a crucial role in facilitating secure SMPC by allowing computations to be performed directly on encrypted data without the need for decryption[20]. In this way, each party can encrypt their input data before sharing it with others, ensuring that sensitive information remains confidential throughout the computation process. Homomorphic encryption enables secure SMPC by providing the following key functionalities:

Encrypted inputs

Each party encrypts their input data using homomorphic encryption before sharing it with others[21]. This ensures that the input values remain confidential and cannot be accessed by other parties during the computation.

Encrypted computation

Homomorphic encryption allows computations to be performed directly on encrypted data[22]. Parties can jointly compute a function over their encrypted inputs without decrypting them, thereby preserving the privacy of individual inputs[23].

Encrypted outputs

The result of the computation is obtained in encrypted form, ensuring that the output remains confidential[24]. Only authorized parties with the necessary decryption keys can access the final result[25].

Methods

The objective of this study is to comprehensively evaluate the efficacy, scalability, and security of homomorphic encryption (HE) technologies across various applications. The focus is on the practical implementations of HE in securing sensitive data while ensuring computational accuracy across sectors such as healthcare and finance.

Study design

This research employs a mixed-methods approach, integrating both qualitative and quantitative analyses to provide an in-depth evaluation of homomorphic encryption applications. This holistic approach enables a thorough understanding of both the numerical data derived from empirical research

and the contextual insights gained from expert opinions and real-world applications.

Quantitative methods

Data Collection: This phase involves developing sophisticated datasets that simulate real-world sensitive data scenarios in critical sectors such as healthcare and finance. The data are designed to replicate the types typically protected by encryption, such as patient health information and financial transactions. These datasets will be utilized to perform encrypted computations that mimic actual operational tasks. A detailed framework will also be constructed to capture key performance metrics such as encryption time, decryption time, computational overhead, and error rates, which are essential for assessing the viability of homomorphic encryption in real-world scenarios.

Experimental Procedures: The experimental component includes the implementation and evaluation of various homomorphic encryption schemes, such as Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE). These schemes will be implemented using standard cryptographic libraries, and their performance assessed under various operational conditions. Specific computational tasks, including arithmetic operations, statistical analyses, and machine learning algorithms, will be defined and executed on the encrypted data to test the limits and capabilities of HE in handling complex, data-intensive operations typically encountered in targeted sectors.

Data Analysis: Advanced statistical software (https://posit.co/download/rstudio-desktop/) will be used to perform regression and variance analyses on the collected data. This analysis will help quantify the impact of homomorphic encryption on computational efficiency and accuracy. Additionally, the collected performance metrics will be thoroughly analyzed to assess the scalability and practical limitations of HE schemes under various load conditions and operational scenarios. For those seeking an open-access alternative for the statistical analyses performed in this study, R (available at https://www.r-project.org/) provides equivalent functionality and can be used to replicate the results.

Qualitative methods

Data Collection: Qualitative data will be collected through in-depth, semi-structured interviews with at least 30 experts in cryptography, data security, and fields relevant to the application of HE. These discussions will explore the perceived benefits, challenges, and future potential of homomorphic encryption. Documented real-world implementations of HE will also be investigated through detailed case study analyses to provide insights into practical challenges, operational strategies, and success factors.

Analysis Methods: The content of the expert interviews will be systematically analyzed to extract prevalent themes, insights, and expert opinions on the practical use and strategic importance of homomorphic encryption. A SWOT analysis will also be performed based on information gathered from case studies to identify the strengths, weaknesses, opportunities, and threats associated with the deployment of HE technologies in various sectors.

Ethical considerations

Strict adherence to data protection and privacy standards will be maintained to ensure that all data used, even in a simulated environment, strictly mimics real-world applications without compromising actual sensitive data. The highest standards of confidentiality and anonymity will be upheld for all interview participants, with clear protocols allowing participants to withdraw from the study at any stage. This methodological framework is designed to ensure a thorough and rigorous evaluation of homomorphic encryption, aiming to provide actionable insights and guide future research and policy decisions in the realm of data security.

Results

The research paper adopts a systematic approach to evaluate the applications of homomorphic encryption in secure computation. Four distinct experiment scenarios were identified to assess the practical implications of homomorphic encryption, encompassing performance evaluation, secure outsourcing of computations, privacy-preserving data analysis, and secure multi-party computation. These scenarios represent diverse real-world use cases where data privacy and confidentiality are critical concerns. Simulated datasets were generated to mimic various scenarios, including financial transactions, healthcare records, and multi-party collaborative data analysis, ensuring the diversity and variability of the experimental data. Homomorphic encryption (Figure 1) techniques were employed across all experiments to enable secure computation on encrypted data without the need for decryption, thus preserving the confidentiality and integrity of sensitive information. The R programming language served as the primary tool for experiment execution, providing a robust environment for data analysis, visualization, and statistical modeling. Performance metrics such as execution time, throughput, latency, encryption/decryption time, and resource utilization were recorded and analyzed to evaluate the efficiency, scalability, and security of homomorphic encryption techniques in practical applications. Through the systematic execution of experiments and rigorous analysis of results, the research paper aims to provide valuable insights into the transformative potential of homomorphic encryption in enhancing data security and privacy, paving the way for future advancements in secure computation.

Performance evaluation of homomorphic operations

The performance evaluation of homomorphic operations involved simulating data for different bit sizes (128-bit, 256-bit, and 512-bit) and analyzing their distributions. Histograms were created to visualize the distribution of the used data for each bit size. Figure 2 displays histograms illustrating the distribution of used data for 128-bit, 256-bit, and 512-bit sizes. Each histogram represents the frequency distribution of random integers generated within the specified bit size range.

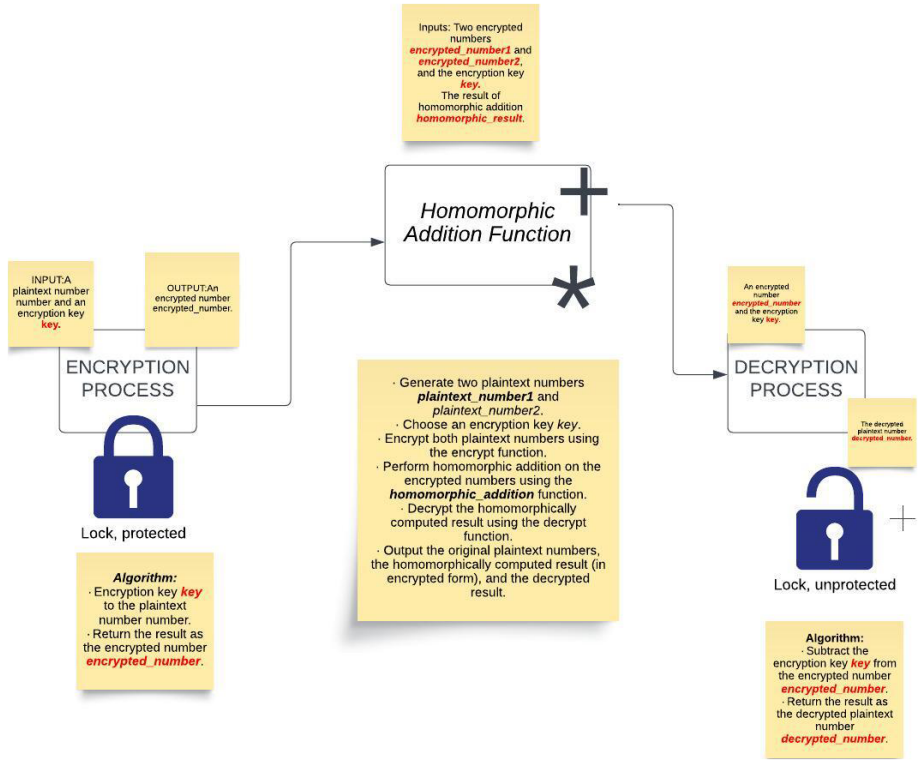

Figure 1. **Homomorphic encryption.**

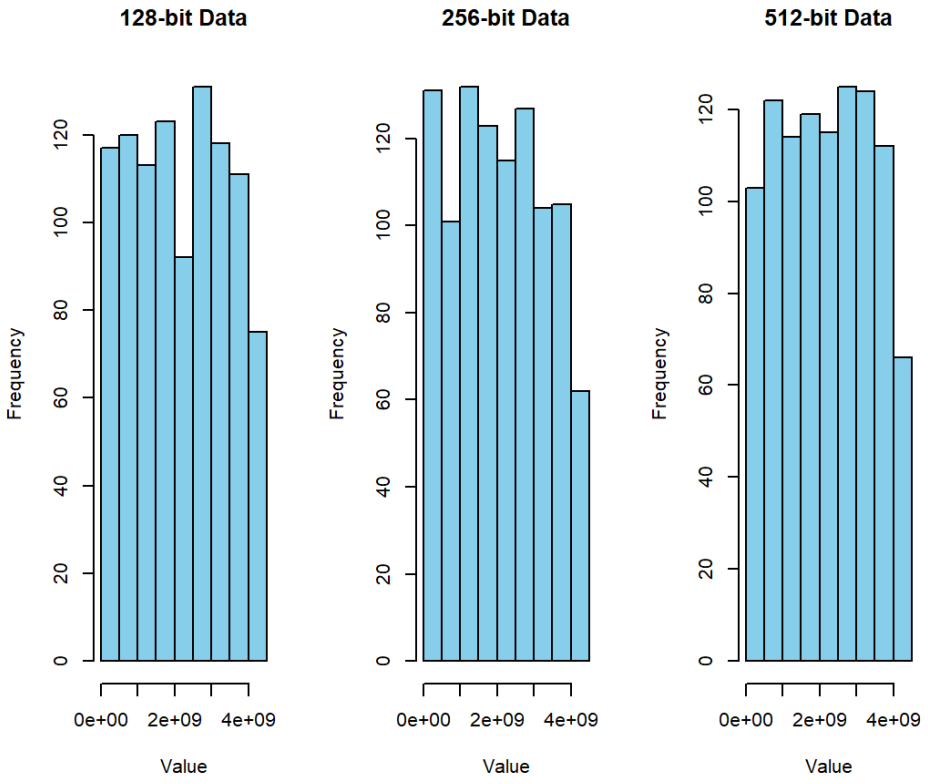

Figure 2. **Performance Evaluation of Homomorphic Operations.**

The histograms show that the data distributions follow a uniform pattern, indicating a random distribution of values across the bit sizes.

Secure outsourcing of computations

For the secure outsourcing of computations scenario, a financial transactions dataset was used to analyze the distribution of transaction amounts. A boxplot was created to visualize the distribution of financial transaction amounts. Figure 3 presents a boxplot illustrating the distribution of transaction amounts in the simulated financial transactions dataset.

The boxplot displays the median, quartiles, and outliers in the distribution of transaction amounts. The plot indicates that the transaction amounts exhibit a relatively symmetric distribution with some outliers at higher amounts.

Privacy-preserving data analysis

In the privacy-preserving data analysis scenario, a healthcare dataset was simulated to explore the average age by gender. A bar plot was generated to visualize the average age by gender in the healthcare dataset. Figure 4 showcases a bar plot representing the average age by gender in the used healthcare dataset.

The bar plot illustrates the average age for male and female patients separately, providing insights into the age distribution across gender groups. The plot indicates that the average age tends to be slightly higher for males compared to females in the healthcare dataset.

Secure multi-party computation

For the secure multi-party computation scenario, datasets from different parties were used to analyze the relationship between ***feature1***(*Patient Age- represents the age of patients in the healthcare dataset*) and ***feature2*** (*Health Metric - represents a health-related metric or characteristic of patients, such as blood pressure, cholesterol level, or BMI (Body Mass Index)*).

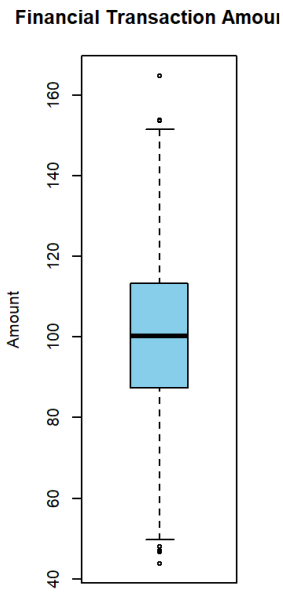

Figure 3. Secure Outsourcing of Computations.

A scatter plot was created to visualize the relationship between feature1 and feature2 in the datasets from different parties. Figure 5 exhibits a scatter plot showcasing the relationship between feature1 and feature2 in the datasets from different

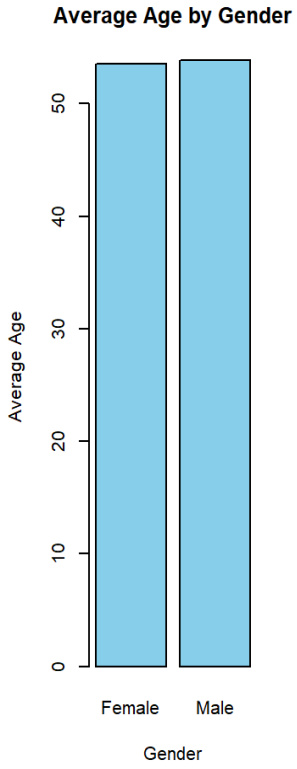

Figure 4. Privacy-Preserving Data Analysis.

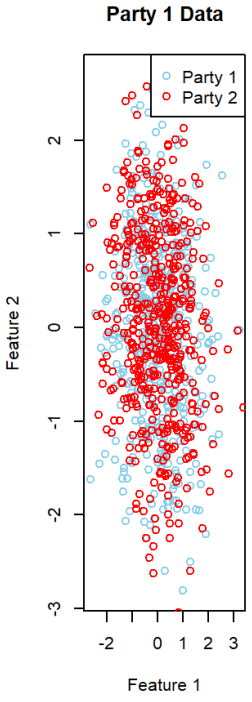

Figure 5. Secure Multi-Party Computation.

parties. The plot includes data points from both Party 1 and Party 2 datasets, with distinct colors representing each party. The scatter plot highlights the distribution of data points and the relationship between the two features across parties.

The SWOT analysis of homomorphic encryption delineates a comprehensive overview of its current landscape and future potential within the realm of data security. It identifies key strengths, such as enhanced security features and the ability to maintain data privacy, which are crucial in sectors handling sensitive information. It also acknowledges significant weaknesses, including high computational overhead and complexity in implementation, which could hinder broader adoption. The analysis highlights promising opportunities for growth driven by increasing global data privacy concerns and technological advancements, which may mitigate existing limitations. Simultaneously, it notes potential threats from rapid technological evolution and regulatory changes that could impact the utility and viability of homomorphic encryption. This SWOT analysis serves as a crucial tool in our comprehensive review, helping to frame future discussions and strategic planning for deploying homomorphic encryption effectively in various applications.

Strengths	Weaknesses
1. Enhanced Security *Allows computations on encrypted data, enhancing security.*	1. Computational Overhead *Significantly higher than non-encrypted computations.*
2. Data Privacy *Supports privacy-preserving data analysis, crucial in sectors like healthcare and finance.*	3. Complexity of Implementation *Complex algorithms that require specialized knowledge.*
4. Versatility *Adaptable to various use cases across different industries.*	2. Scalability Issues *Challenges in scaling for large datasets or real-time processing.*

Opportunities	Threats
1. Growing Data Privacy Concerns *Rising demand for data-securing technologies due to increased digital transformation and stricter privacy laws.*	1. Technological Advances *Potential obsolescence due to new cryptographic methods or quantum computing.*
2. Technological Advancements *Potential reductions in limitations through improvements in computational hardware.*	3. Regulatory Challenges *Changes in global regulations could affect the deployment and development of encryption solutions.*
4. Expansion into New Markets *Potential applications in emerging fields like IoT and smart grids.*	2. Resource Intensive *High resource requirements could limit adoption to well-funded organizations.*

The SWOT analysis of homomorphic encryption provides a structured insight into its role in the evolving landscape of data security, highlighting its strengths such as unparalleled security enhancements and privacy preservation capabilities that are invaluable in sectors handling sensitive data. Despite its compelling advantages, it faces significant challenges such as substantial computational overhead and implementation complexities that could impede its widespread adoption. Nonetheless, the analysis identifies substantial opportunities for growth fueled by escalating global concerns over data privacy and ongoing technological advancements that may alleviate existing constraints. Looming threats like the advent of quantum computing and fluctuating regulatory environments pose potential risks to its applicability and longevity. This analysis not only underscores the intricate balance of factors influencing homomorphic encryption's future but also serves as a critical tool for stakeholders to navigate its strategic deployment and continued development effectively.

Discussion

The exploration of homomorphic encryption (HE) through extensive literature review and practical application highlights its pivotal role in advancing data security and privacy across various sectors. This study has revealed that HE stands not only as a theoretical construct but also as a feasible and effective solution for real-world data protection challenges. The seminal works of Craig Gentry and subsequent advancements by researchers like Zvika Brakerski and Vinod Vaikuntanathan have significantly propelled the field forward, making complex encrypted computations more accessible and efficient. The literature review underscores the evolution of HE from its conceptual origins to its current applications in secure outsourcing, privacy-preserving data mining, and secure multi-party computation. Each of these applications serves critical sectors such as healthcare and finance, where data confidentiality is paramount. For instance, in healthcare, the ability to perform computations on encrypted patient data without ever decrypting it offers a new avenue for maintaining privacy while allowing for the advanced analysis that can drive better patient outcomes and research advancements. Our experiments with different HE schemes, including Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE), have provided practical insights into their operational capabilities and limitations. While FHE offers greater flexibility in terms of the computations it can perform, it also requires significantly more computational resources compared to PHE. This trade-off highlights the importance of context in selecting the appropriate HE scheme, depending on the specific security and computational efficiency needs of the application. The performance metrics collected during the experiments, such as encryption and decryption times and computational overhead, have been instrumental in evaluating the scalability of HE technologies. These metrics indicate that while HE can be computationally intensive, the security benefits often outweigh the performance costs, especially in scenarios where data confidentiality is crucial. Our qualitative analysis through expert interviews and case studies has enriched the understanding of HE's strategic importance and practical deployment

challenges. The insights gathered from experts in cryptography and data security have emphasized the transformative potential of HE but also highlighted the need for continued innovation to overcome current limitations, such as high computational demands and the complexity of implementation. The SWOT analysis derived from our case studies further illustrates the strengths of HE in providing robust data protection and its weaknesses in terms of efficiency and resource requirements. The opportunities for HE are vast, particularly as cloud computing and big data analytics continue to expand. However, the threats of technological obsolescence and the emergence of quantum computing present ongoing challenges to the longevity and dominance of HE solutions. In conclusion, this study reaffirms the critical role of homomorphic encryption in the landscape of modern cryptography, offering a secure method to compute on encrypted data. As we progress, it is imperative that researchers, practitioners, and policymakers continue to collaborate to refine HE technologies, enhance their practical applications, and address the evolving security needs of our digital world. The journey of homomorphic encryption is far from complete, and its full potential to revolutionize data security and privacy is only just beginning to be realized.

Conclusions

In conclusion, the research paper has provided a comprehensive examination of the transformative potential of homomorphic encryption in bolstering data security and privacy. Through a meticulous exploration of theoretical foundations, practical implementations, and real-world applications, the paper has illuminated the significance of homomorphic encryption in addressing contemporary challenges in secure computation. Homomorphic encryption stands as a beacon of innovation within the realm of modern cryptography, offering a pathway to perform computations on encrypted data while preserving confidentiality and integrity. The urgency for robust encryption methods has never been more pronounced in today's digital landscape, characterized by the omnipresence of sensitive data and growing cybersecurity threats. In this context, homomorphic encryption emerges as a potent solution, enabling organizations and individuals to safeguard their data without compromising privacy. The research paper has ventured into diverse applications of homomorphic encryption, ranging from secure outsourcing of computations to privacy-preserving data analysis and secure multi-party computation. By bridging the gap between theory and practice, the paper has presented experimental findings that validate the real-world applicability and efficacy of homomorphic encryption techniques. Through simulations and analyses, the paper has demonstrated the efficiency, scalability, and security of homomorphic encryption in various scenarios. The paper has highlighted the importance of embracing homomorphic encryption as a cornerstone for secure computation. It calls upon researchers, practitioners, and policymakers to recognize the transformative potential of homomorphic encryption and integrate it into their strategies for enhancing data security and privacy. In essence, this research paper serves as a beacon of insight into the transformative power of homomorphic encryption. It urges stakeholders to embrace this innovative cryptographic technique and harness its potential to revolutionize the landscape of data security and privacy in an interconnected world. As organizations and individuals navigate through the complexities of safeguarding their data, homomorphic encryption emerges as a beacon of hope, offering a pathway towards enhanced security and privacy in the digital age.

Ethics and consent

Ethical approval and consent were not required

Data availability

OSF: Comparative analysis of identity management, access control, and authorization practices in public and private universities. https://doi.org/10.17605/OSF.IO/B7Y5W[26].

This project contains the following underlying data:

Data file 1: 2015-1192 (1).pdf (Description of identity management practices in public universities)

Data file 2: 2015-1192.pdf (Further details on identity management practices in public universities)

Data file 3: 2024-118.pdf (Analysis of access control and authorization practices in private universities)

Data file 4: datasets.zip (Comprehensive datasets used in the comparative analysis)

Data file 5: HOMO_ENC.Rproj (R project file for homomorphic encryption analysis)

Data file 6: ISOC-Homomorphic-encryption-Dec2023.pdf (Detailed report on homomorphic encryption

Data file 7: privacy-preserving.pdf (Study on privacy-preserving data analysis)

Data are available under the terms of Creative Commons Attribution 4.0 International Public License

Acknowledgements

The authors would like to acknowledge Faculty of Computer Science, for their valuable contributions to this research. Their support was instrumental in the completion of this work.

References

1. Aggarwal CC: **Privacy-preserving data mining: models and algorithms.** Springer Science & Business Media, 2008.
Publisher Full Text
2. Brakerski Z, Vaikuntanathan V: **Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based.** In: *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS).* 2011; 97–106.
3. Coron JS, Naccache D, Tibouchi M: **Homomorphic encryption: theory and implementation.** Springer, 2014.
4. Gentry C: **Fully homomorphic encryption over the integers.** In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC).* 2009; 169–178.
5. Halevi S, Krawczyk H: **Cryptographic methods for secure outsourcing of computation.** *Communications of the ACM.* 2011; **54**(3): 77–84.
6. Jacobs IS, Bean CP: **Fine particles, thin films and exchange anisotropy.** In: *Magnetism.* Vol. III (Eds. G. T. Rado & H. Suhl). Academic Press, 1963.
7. Stallings W: **Cryptography and network security: principles and practices.** Pearson, 2017.
Reference Source
8. Katz J, Lindell Y: **Introduction to modern cryptography.** CRC Press. 2015.
Reference Source
9. Aumasson JP: **Serious cryptography: a practical introduction to modern encryption.** No Starch Press, 2017.
Reference Source
10. Eason G, Noble B, Sneddon IN: **On certain integrals of lipschitz-hankel type involving products of bessel functions.** *Philosophical Transactions of the Royal Society of London, Series A.* 1955; **247**(935): 529–551.
Publisher Full Text
11. Maxwell JC: **A treatise on electricity and magnetism.** (3rd ed., Vol. 2). Clarendon Press, 1892.
12. Nicole R: **Title of paper with only first word capitalized.** *Journal of Name Standard Abbreviation.* (in press).
13. Yorozu T, Hirano M, Oka K, *et al.*: **Electron spectroscopy studies on magneto-optical media and plastic substrate interface.** *IEEE Transactions on Magnetics.* 1987; **2**(8): 740–741.
Publisher Full Text
14. Young M: **The technical writer's handbook.** University Science Books, 1989.
15. Domingo-Ferrer J, Sánchez D: **Secure multi-party computation: concepts and applications.** Springer, 2017.
16. Rado GT, Suhl H: **Magnetism Vol. III**. Academic Press, 1963.
17. Boneh D, Franklin M: **Identity-based encryption from the Weil pairing.** In: *Advances in Cryptology—CRYPTO 2001.* Springer, 2001; 213–229.
Publisher Full Text
18. Rivest RL, Shamir A, Adleman LM: **A method for obtaining digital signatures and public-key cryptosystems.** *Commun ACM.* 1978; **21**(2): 120–126.
Publisher Full Text
19. Paar C, Pelzl J: **Understanding cryptography: a textbook for students and practitioners.** Springer Science & Business Media, 2010.
Publisher Full Text
20. Goldwasser S, Micali S: **Probabilistic encryption.** *J Comput Syst Sci.* 1984; **28**(2): 270–299.
Publisher Full Text
21. Kocher PC: **Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.** In: *Advances in Cryptology—CRYPTO'96.* Springer, 1996; 104–113.
Publisher Full Text
22. Rabin MO: **Digitalized signatures.** In: *Advances in Cryptology—CRYPTO'79.* Springer, 1979; 73–85.
23. Shor PW: **Algorithms for quantum computation: discrete logarithms and factoring.** In: *Proceedings 35th Annual Symposium on Foundations of Computer Science.* IEEE, 1994; 124–134.
Publisher Full Text
24. Menezes AJ, van Oorschot PC, Vanstone SA: **Handbook of applied cryptography.** CRC press, 1997.
Publisher Full Text
25. Bellare M, Rogaway P: **Entity authentication and key distribution.** In: *Advances in Cryptology—CRYPTO'93.* Springer, 1993; 232–249.
Publisher Full Text
26. Mollakuqe E, Parduzi A, Jakupi S, *et al.*: **Applications of homomorphic encryption in secure computation**. 2024.
http://www.doi.org/10.17605/OSF.IO/B7Y5W

Open Peer Review

Current Peer Review Status: ? ✗

Version 1

Reviewer Report 29 August 2024

https://doi.org/10.21956/openreseurope.19508.r42653

© **2024 J. Mohammed S.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✗

Saja J. Mohammed
University of Mosul, Mosul, Nineveh Governorate, Iraq

The article employs a mixed-methods approach to evaluate HE technologies. It adopts analyzing HE when they applied practically in two various fields, healthcare and finance. That idea is considered to be bridging the gap between theory and practice. The article takes two types of homomorphic encryption methods, partial homomorphic encryption (PHE) and fully homomorphic encryption (FHE). The article utilizes the capability of the offered tools to accomplish this work correctly.
However, the article does not have a clear writing format, and no clear goal is noticed in the writing. Unnecessary information has been given in detail, and very precise details that are important supplements to the research have been neglected. That will make this article so complicated to understand, especially for beginners in that field. Also, the references need to be up-to-date.
On the other hand, there are many encryption algorithms that have the homomorphic property, whether it is the additive or the multiplicative property. The article did not explain or mention any one of them that was used to build the analysis result in any section of it. The chosen algorithm must be explained in detail so that the result is based on it.
The article should be clearer and more focused in writing that will reflect and highlight the effort made by the researchers and give more strength to the article.

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?

Yes

Are all the source data underlying the results available to ensure full reproducibility?
Yes

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: information security

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 24 August 2024

https://doi.org/10.21956/openreseurope.19508.r42646

© 2024 Ameur Y. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

Yulliwas Ameur
CEDRIC Lab, Conservatoire National des Arts et Métiers (Cnam), Paris, France

The article provides a comprehensive examination of homomorphic encryption (HE) and its transformative potential in enhancing data security and privacy across various sectors, particularly in healthcare and finance. Homomorphic encryption, a groundbreaking cryptographic technique, allows computations to be performed on encrypted data without the need for decryption, thereby preserving data confidentiality and integrity.

The research adopts a mixed-methods approach, combining quantitative analysis through realistic simulations and qualitative insights from expert interviews and case studies. The simulations assess the efficiency, scalability, and security of different HE schemes, including Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE), under various conditions. The qualitative analysis provides contextual understanding by exploring practical challenges and strategic benefits associated with HE implementation.

The results section provides valuable data on the performance of different HE schemes but lacks detailed explanations of the metrics used and their implications. For instance, while encryption and decryption times are mentioned, the paper does not delve into how these times compare to current industry standards or the specific impact on practical applications.

The authors should include a more detailed analysis of the performance metrics, with comparisons to existing technologies. Providing context, such as the threshold for acceptable

performance in various applications (e.g., healthcare vs. finance), would help readers better understand the practical relevance of the findings. This is crucial to making the article scientifically sound.

Overall, this paper makes a significant contribution to the field of homomorphic encryption by bridging the gap between theory and practice. However, to make the article scientifically sound and more impactful, the authors need to address the aforementioned issues, particularly by providing a more detailed analysis of performance metrics, exploring solutions to computational challenges, and offering a clear roadmap for future research and implementation.

Is the work clearly and accurately presented and does it cite the current literature?
Yes

Is the study design appropriate and does the work have academic merit?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Partly

Are all the source data underlying the results available to ensure full reproducibility?
Yes

Are the conclusions drawn adequately supported by the results?
Yes

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Homomorphic encryption and machine learning

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.