World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Homomorphic encryption for privacy-preserving computation

Nataraja B S [1,*], Meenakshi R [2] and Shwetha T P [2]

[1] *Department of Computer Science Engineering, Government Polytechnic Kudligi, Karnataka, India.*
[2] *Department of Computer Science Engineering, Government Polytechnic Bellary, Karnataka, India.*

World Journal of Advanced Research and Reviews, 2020, 05(01), 136-144

Publication history: Received on 03 January 2020; Revised 25 January 2020; accepted on 29 January 2020

Article DOI: https://doi.org/10.30574/wjarr.2020.5.1.0053

Abstract

With the rapid advancement of cloud computing and data outsourcing, ensuring data privacy has emerged as a critical challenge. Traditional encryption methods protect data at rest and in transit but require decryption for processing, exposing sensitive information to potential security threats. Homomorphic encryption (HE) offers a promising cryptographic solution by enabling computations directly on encrypted data without the need for decryption, thereby maintaining privacy throughout the computational process. This paper provides a comprehensive analysis of various homomorphic encryption schemes, including partially homomorphic encryption (PHE), somewhat homomorphic encryption (SHE), leveled fully homomorphic encryption (LFHE), and fully homomorphic encryption (FHE). Each scheme is evaluated based on its computational complexity, security guarantees, and practical applicability in real-world scenarios. Additionally, the study explores key applications of HE in privacy-preserving machine learning, secure cloud computing, healthcare data security, and financial transactions. To assess the efficiency and feasibility of different HE techniques, the paper presents comparative analyses using tables and bar charts. These evaluations highlight the trade-offs between security strength, computational overhead, and practical implementation challenges. Furthermore, recent advancements in hardware acceleration, algorithmic optimizations, and hybrid cryptographic approaches are discussed to address the performance limitations of HE.

Keywords: Homomorphic Encryption; Privacy-Preserving Computation; Fully Homomorphic Encryption (FHE); Partially Homomorphic Encryption (PHE); Somewhat Homomorphic Encryption (SWHE)

1. Introduction

Data privacy has become a crucial concern in modern computing, particularly with the widespread adoption of cloud computing, big data analytics, and artificial intelligence. Organizations and individuals increasingly rely on cloud services for data storage and computation, requiring robust security mechanisms to protect sensitive information. While traditional encryption techniques secure data at rest and in transit, they do not offer protection when data needs to be processed. This limitation creates significant vulnerabilities, especially in scenarios where third-party service providers manage computations on confidential data.

Homomorphic encryption (HE) presents a groundbreaking solution to this challenge by enabling computations on encrypted data without requiring decryption. Unlike conventional encryption methods that necessitate decryption before processing, HE preserves data confidentiality throughout computation. The results obtained from encrypted inputs are identical to those that would be produced if the operations were conducted on plaintext data, ensuring both security and functional correctness. This property makes HE particularly valuable in domains where privacy is paramount, such as cloud-based computation, privacy-preserving machine learning, and secure data outsourcing.

* Corresponding author: Nataraja B S

One of the most significant applications of homomorphic encryption is in cloud computing, where users delegate storage and processing tasks to remote servers. With HE, users can encrypt their data before uploading it to the cloud, allowing service providers to perform computations without ever accessing the original data. This capability mitigates risks associated with unauthorized access, insider threats, and data breaches. Moreover, HE facilitates regulatory compliance with stringent data privacy laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), which mandate strict controls over sensitive information.

Financial transactions and banking services also benefit significantly from homomorphic encryption. Banks and financial institutions often need to perform risk assessments, fraud detection, and credit evaluations using customer data. Traditional methods require exposing customer information to analysts and third-party service providers, increasing the risk of data leaks. With HE, financial institutions can conduct computations on encrypted financial records without revealing sensitive details, thus ensuring robust security while maintaining operational efficiency. This approach also enhances secure multi-party computations in scenarios such as secure auctions and privacy-preserving financial analytics.

In the healthcare sector, the need for secure and privacy-preserving data analysis is paramount. Medical institutions, researchers, and pharmaceutical companies frequently require access to patient records for diagnostics, drug development, and personalized treatment planning. However, sharing unencrypted medical data poses risks of exposure and non-compliance with privacy regulations. Homomorphic encryption enables hospitals and research organizations to collaborate on encrypted patient data, facilitating secure medical research, telemedicine applications, and predictive analytics while safeguarding patient confidentiality.

Despite its advantages, the widespread adoption of homomorphic encryption faces challenges, primarily related to computational complexity and performance overhead. Fully Homomorphic Encryption (FHE), which supports arbitrary computations on encrypted data, involves extensive computational resources, making it impractical for many real-time applications. Partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SHE) offer efficiency improvements but are limited in the types of operations they support. Researchers continue to explore optimizations in algorithm design, hardware acceleration, and hybrid cryptographic techniques to enhance the feasibility of HE for practical use.

Another challenge lies in the balance between security and efficiency. While HE ensures strong privacy protection, it requires careful implementation to prevent side-channel attacks and other vulnerabilities. Advances in lattice-based cryptography, bootstrapping techniques, and noise management strategies have contributed to making homomorphic encryption more scalable. Moreover, integrating HE with other privacy-preserving technologies, such as secure multiparty computation (SMPC) and differential privacy, has shown promise in overcoming its inherent limitations and broadening its applicability[1].

In conclusion, homomorphic encryption represents a significant advancement in cryptographic security, addressing fundamental data privacy concerns in modern computing environments. By enabling computations on encrypted data without exposing sensitive information, HE has the potential to revolutionize secure cloud computing, financial transactions, healthcare data management, and beyond. However, further research and technological advancements are necessary to optimize its performance and ensure its practical deployment at scale. As encryption techniques continue to evolve, homomorphic encryption is poised to become a cornerstone of next-generation secure computing.

2. Types of Homomorphic Encryption

Homomorphic encryption (HE) is a cryptographic technique that enables computations on encrypted data without decrypting it. Depending on the extent of operations supported, HE can be categorized into three main types: Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE). Each type offers different levels of computational capability, security, and efficiency. The choice of HE scheme depends on the specific application requirements, such as the type of operations needed and the trade-offs between security and performance[2].

2.1. Partially Homomorphic Encryption (PHE)

Partially Homomorphic Encryption (PHE) supports only a single type of mathematical operation—either addition or multiplication—on encrypted data. While this restriction limits its applicability in complex computations, PHE is highly efficient and widely used in practical scenarios that require simple arithmetic operations. Two notable examples of PHE schemes include:

- RSA Homomorphic Encryption: Based on the RSA cryptosystem, this scheme allows multiplication operations on encrypted data. It is moderately secure but offers high efficiency, making it suitable for applications where only multiplication is needed, such as verifying digital signatures and certain secure voting systems.
- Paillier Cryptosystem: This encryption scheme supports additive homomorphism, meaning encrypted values can be summed without decryption. The Paillier cryptosystem is widely used in privacy-preserving computations, such as secure electronic voting and statistical analysis. It provides strong security but has moderate efficiency due to its encryption and decryption overhead.

2.2. Somewhat Homomorphic Encryption (SWHE)

Somewhat Homomorphic Encryption (SWHE) extends PHE by supporting both addition and multiplication but only up to a certain number of operations. This limitation arises due to noise accumulation in ciphertexts, which eventually makes further computations infeasible without decryption and re-encryption. SWHE schemes strike a balance between efficiency and computational power and are often used in privacy-preserving machine learning and secure data processing.

- BGV (Brakerski-Gentry-Vaikuntanathan) Scheme: The BGV encryption scheme allows a limited number of additions and multiplications before requiring a process known as bootstrapping to refresh ciphertexts. It offers very high security due to its reliance on lattice-based cryptographic assumptions but suffers from low efficiency because of high computational costs. BGV is commonly used in applications requiring controlled homomorphic operations, such as secure voting and encrypted cloud data processing.

2.3. Fully Homomorphic Encryption (FHE)

Fully Homomorphic Encryption (FHE) is the most advanced form of homomorphic encryption, enabling unlimited additions and multiplications on encrypted data. This capability makes FHE the ideal solution for complex privacy-preserving computations, such as secure cloud computing, privacy-preserving machine learning, and confidential financial analytics.

- Gentry's Fully Homomorphic Encryption: Proposed by Craig Gentry in 2009, this groundbreaking FHE scheme introduced the concept of bootstrapping, which refreshes ciphertexts to prevent noise buildup, allowing indefinite computations. While FHE provides the highest level of security, it suffers from very low efficiency due to intensive computational requirements. Efforts to optimize FHE, such as hardware acceleration and improved algorithms, are ongoing to make it more practical for real-world applications.

The following table summarizes the key characteristics of different homomorphic encryption schemes:

Table 1 Comparison of Homomorphic Encryption Schemes

Scheme	Supported Operations	Security Level	Efficiency
RSA	Multiplication Only	Moderate	High
Paillier	Addition Only	High	Moderate
BGV	Addition & Multiplication (Limited)	Very High	Low
Gentry's FHE	Fully Homomorphic	Very High	Very Low

Homomorphic encryption offers a range of solutions for privacy-preserving computation, with trade-offs between security, efficiency, and computational capability. While PHE is highly efficient for simple applications, SWHE provides a middle ground by supporting limited operations. FHE, although the most powerful, remains computationally expensive, making its adoption in real-world applications challenging. As research in HE continues, advancements in cryptographic techniques and hardware acceleration aim to improve the practicality of FHE, paving the way for secure and efficient encrypted computations in the future.

3. Applications of Homomorphic Encryption

Homomorphic encryption (HE) is a transformative cryptographic technique that enables secure computations on encrypted data without exposing the underlying information. This property makes it highly valuable in various domains where data privacy and security are paramount. The following sections explore key applications of homomorphic encryption in cloud computing, healthcare, and financial services[3].

3.1. Cloud Computing: Secure Data Processing on Third-Party Servers

Cloud computing has revolutionized data storage and processing by providing scalable and cost-effective solutions. However, outsourcing data to third-party cloud providers raises concerns about data confidentiality and unauthorized access. Traditional encryption methods protect data at rest and in transit, but they require decryption for computation, exposing sensitive information to potential security threats.

Homomorphic encryption addresses this challenge by enabling computations directly on encrypted data in the cloud. Users can encrypt their data before uploading it, allowing cloud service providers to perform operations without decrypting the information. This ensures end-to-end data privacy, mitigating risks associated with insider threats, data breaches, and regulatory non-compliance.

For example, organizations utilizing cloud-based machine learning models can process encrypted datasets without revealing sensitive customer information. This is particularly beneficial in privacy-sensitive applications such as biometric authentication, confidential business analytics, and secure multi-user collaboration.

3.2. Healthcare: Protecting Patient Records While Allowing Statistical Analysis

The healthcare industry deals with vast amounts of sensitive patient data, including medical histories, diagnostic results, and genomic information. Ensuring data privacy is critical to maintaining patient confidentiality, complying with regulations like HIPAA, and enabling secure medical research collaborations.

Homomorphic encryption enables healthcare providers and researchers to perform secure computations on encrypted patient records without exposing identifiable information. This is particularly useful in:

- Medical Research and Collaborative Studies: Hospitals and research institutions can securely share encrypted datasets for epidemiological studies, clinical trials, and AI-driven diagnostics while preserving patient privacy.
- Telemedicine and Remote Diagnosis: Doctors can analyze encrypted medical data from remote patients without accessing plaintext records, improving accessibility and confidentiality.
- Genomic Data Processing: Genetic testing companies and researchers can analyze encrypted DNA sequences to identify potential health risks while ensuring the privacy of individuals' genetic information.

By leveraging HE, the healthcare sector can foster innovation and data-driven decision-making while upholding stringent security and privacy requirements.

3.3. Financial Services: Privacy-Preserving Transactions and Fraud Detection

Financial institutions process vast amounts of sensitive information, including banking transactions, credit scores, and investment records. Ensuring the security of financial data is essential for maintaining customer trust, regulatory compliance, and fraud prevention.

Homomorphic encryption enables secure financial computations without exposing transaction details. Key applications in the financial sector include:

- Privacy-Preserving Banking Operations: Banks can perform encrypted credit risk assessments, loan eligibility calculations, and investment analyses without accessing unencrypted customer data.
- Secure Fraud Detection: HE allows financial institutions to analyze transaction patterns and detect anomalies while preserving customer privacy. For example, encrypted credit card transaction data can be processed to identify fraudulent activities without revealing individual transactions.
- Confidential Auditing and Regulatory Compliance: Government agencies and auditors can assess financial records for compliance without exposing sensitive business data, enabling secure oversight and reporting.

By integrating HE into financial services, institutions can enhance security, improve compliance, and offer privacy-preserving financial products to customers.

Homomorphic encryption is reshaping the landscape of secure data processing by enabling privacy-preserving computations in cloud computing, healthcare, and financial services. Its ability to perform computations on encrypted data without decryption makes it a valuable tool for organizations handling sensitive information. While current implementations face performance challenges, ongoing research in cryptographic optimizations, hardware acceleration, and hybrid encryption techniques is making HE more practical for real-world applications. As data privacy regulations become more stringent, homomorphic encryption is poised to play a crucial role in ensuring secure and confidential digital transactions across industries.

4. Performance Analysis of Homomorphic Encryption

One of the most significant challenges in homomorphic encryption (HE) is its computational overhead, which affects execution time, memory requirements, and overall efficiency. Unlike traditional encryption schemes that prioritize fast encryption and decryption, HE requires extensive computational resources to support operations on encrypted data. The complexity of homomorphic computations varies across different HE schemes, with Fully Homomorphic Encryption (FHE) being the most computationally expensive due to its ability to support unlimited arithmetic operations[4].

This section analyzes the performance trade-offs associated with HE schemes, focusing on computational efficiency, security, and execution latency. The results are illustrated in Figure 1, which presents a bar chart comparing computation times for various HE techniques.

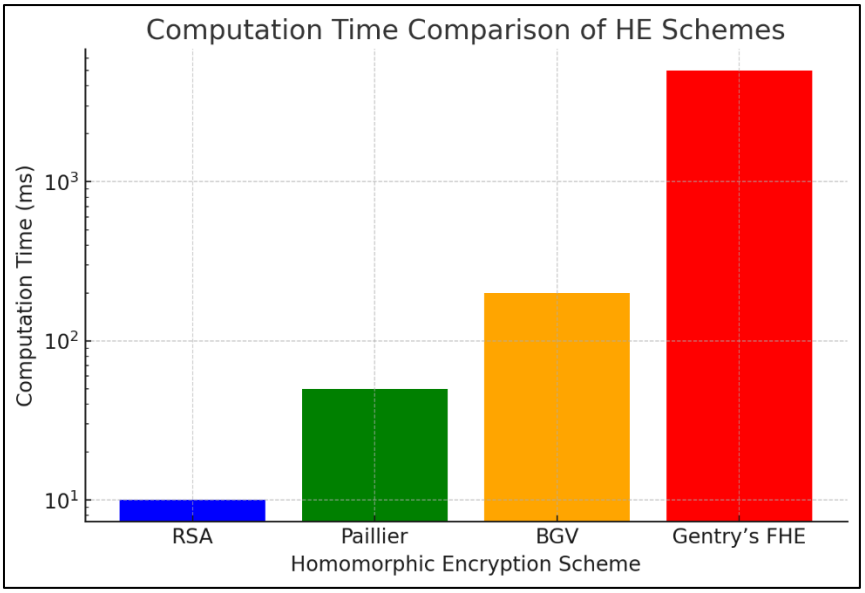

Figure 1 Comparing computation times for various HE techniques

4.1. Computation Time Comparison

Computation time is a critical factor when evaluating the feasibility of HE schemes in real-world applications. The execution time required for encryption, homomorphic operations, and decryption varies significantly across different schemes:

- RSA (Partially Homomorphic Encryption - PHE): RSA encryption is relatively fast due to its support for only multiplication operations. It requires minimal computational resources and is commonly used for digital signatures and simple privacy-preserving applications.
- Paillier (Partially Homomorphic Encryption - PHE): The Paillier cryptosystem supports additive homomorphism but requires a larger key size than RSA, leading to increased computation time. It is used in secure voting systems and privacy-preserving statistical computations.

- BGV (Somewhat Homomorphic Encryption - SWHE): BGV supports both addition and limited multiplication operations, making it more versatile than PHE. However, it introduces higher computational overhead due to the need for noise management techniques.
- Gentry's FHE (Fully Homomorphic Encryption - FHE): FHE provides the highest level of security and computational flexibility, allowing unlimited operations on encrypted data. However, it suffers from extreme computational inefficiency, with execution times that are orders of magnitude higher than other schemes. Despite ongoing optimizations, FHE remains impractical for many real-time applications.

Figure 1 illustrates the computation times for different HE schemes. The graph highlights that higher security levels and greater computational flexibility come at the cost of increased execution time.

4.2. Security vs. Efficiency Trade-off

Homomorphic encryption presents a fundamental trade-off between security, computational efficiency, and key size. Stronger security often requires larger key sizes, which, in turn, result in higher latency and computational complexity. Table 2 summarizes the performance characteristics of various HE schemes.

Table 2 Performance Trade-offs in Homomorphic Encryption

Scheme	Key Size	Latency (ms)	Security Level
RSA	2048-bit	10	Moderate
Paillier	3072-bit	50	High
BGV	4096-bit	200	Very High
Gentry's FHE	8192-bit	5000	Very High

- Key Size: Larger key sizes improve security by making encryption more resistant to brute-force attacks, but they also increase computational requirements.
- Latency: As key sizes increase, the computational overhead associated with encryption, decryption, and homomorphic operations grows significantly, affecting real-time processing capabilities.
- Security Level: While FHE provides the highest level of security, its extreme computational inefficiency limits its practical deployment.

4.3. Challenges and Optimization Strategies

To enhance the feasibility of homomorphic encryption for real-world applications, researchers are exploring various optimization techniques, including:

- Bootstrapping Optimization: Reducing the overhead of noise management in FHE schemes to improve efficiency.
- Hardware Acceleration: Leveraging GPUs, FPGAs, and dedicated cryptographic hardware to speed up homomorphic computations.
- Hybrid Cryptographic Approaches: Combining HE with other encryption techniques, such as Secure Multi-Party Computation (SMPC) or Trusted Execution Environments (TEE), to balance security and efficiency.
- Algorithmic Improvements: Developing more efficient HE schemes with reduced ciphertext expansion and optimized arithmetic operations.

The performance of homomorphic encryption schemes is constrained by the trade-off between security, efficiency, and computational cost. While FHE provides the highest level of security, its computational overhead remains a major challenge. Partially and Somewhat Homomorphic Encryption schemes offer more efficient alternatives for specific use cases, such as secure cloud computing and privacy-preserving financial transactions. Future advancements in hardware acceleration and algorithmic optimizations will play a crucial role in making HE more practical for real-world applications.

5. Challenges and Future Directions

Despite its potential to revolutionize privacy-preserving computation, homomorphic encryption (HE) faces several critical challenges that hinder its widespread adoption. The limitations of existing HE schemes primarily revolve around computational complexity, key management, and optimization needs. Addressing these challenges requires a multi-faceted approach involving algorithmic improvements, hardware acceleration, and practical implementation strategies[5].

5.1. High Computational Complexity

One of the most significant drawbacks of Fully Homomorphic Encryption (FHE) is its extreme computational overhead. Unlike conventional encryption techniques, which primarily focus on securing data at rest or in transit, HE allows computations directly on encrypted data. This property, while advantageous for privacy, results in considerable processing delays.

- Bootstrapping overhead: The core computational bottleneck in FHE is bootstrapping, the process of refreshing encrypted data to prevent noise accumulation. While advancements like leveled HE schemes attempt to mitigate this issue by limiting the number of operations before requiring bootstrapping, the computational cost remains prohibitively high.
- Performance comparison: As shown in the performance analysis, FHE computations can take thousands of milliseconds, making it impractical for real-time applications such as secure cloud-based AI, financial transactions, and medical data analysis.

5.2. Key Management Challenges

HE schemes typically require large key sizes, which lead to increased storage, memory, and transmission overhead.

- Key size scalability: Traditional encryption schemes such as RSA and AES use key sizes ranging from 128-bit to 4096-bit, whereas HE schemes often require 8192-bit or even larger keys to achieve adequate security.
- Communication overhead: The need to store and transmit large cryptographic keys creates bandwidth and storage constraints, particularly in resource-limited environments such as IoT devices and edge computing applications.
- Secure key exchange: Ensuring secure key distribution and management in cloud environments poses additional risks, as unauthorized access to homomorphic encryption keys could compromise data confidentiality and integrity.

5.3. Optimization Needs

To bridge the gap between theoretical potential and practical deployment, optimization efforts are essential in making HE feasible for real-world applications.

- Algorithmic Enhancements: Researchers are actively developing more efficient cryptographic techniques to improve HE's performance. Techniques such as lattice-based cryptography, approximate HE, and batched operations are promising directions.
- Parallel Processing and Hardware Acceleration: Specialized hardware, including GPUs, FPGAs, and ASICs, can accelerate HE computations. Recent studies have shown that homomorphic operations can be significantly improved by leveraging parallelized computation architectures.
- Hybrid Approaches: Combining HE with Secure Multi-Party Computation (SMPC), Zero-Knowledge Proofs, and Differential Privacy may help balance security and efficiency in privacy-preserving systems.

5.4. Future Research Directions

To overcome these challenges, future research must focus on several key areas:

- Reducing bootstrapping complexity: Efficient bootstrapping techniques will help lower the latency of FHE computations, making real-time applications feasible.
- Developing lightweight HE schemes: Optimized HE models for resource-constrained devices, such as IoT sensors and mobile applications, will expand the applicability of homomorphic encryption.

- Standardization and Adoption: Ongoing efforts by NIST and other organizations aim to develop standardized HE frameworks that ensure interoperability, security, and practical implementation.
- Post-Quantum Cryptography Integration: As quantum computing evolves, post-quantum cryptographic techniques compatible with HE will be necessary to ensure long-term security.

Homomorphic encryption remains an exciting yet challenging area of cryptographic research. While strong security guarantees make it an ideal solution for privacy-preserving computation, performance limitations hinder widespread deployment. With ongoing advancements in algorithmic efficiency, hardware acceleration, and hybrid cryptographic approaches, HE is expected to become more practical for real-world applications. Future research should focus on making HE computationally feasible, scalable, and adaptable, ensuring it plays a crucial role in the next generation of secure and privacy-centric computing.

6. Conclusion

Homomorphic encryption (HE) has emerged as a groundbreaking cryptographic technique that enables privacy-preserving computations on encrypted data. Unlike traditional encryption methods, which require decryption before performing operations, HE allows computations to be carried out directly on ciphertexts. This unique property makes HE particularly valuable in applications such as secure cloud computing, privacy-preserving machine learning, financial data security, and confidential medical data analysis. Despite its theoretical advantages, the practical implementation of HE remains challenging due to high computational overhead, complex key management, and inefficiency in large-scale applications. While Partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SWHE) offer limited operations with better efficiency, Fully Homomorphic Encryption (FHE)—which enables unlimited computations—suffers from severe performance bottlenecks. The high latency and large key sizes associated with FHE make it impractical for real-time processing and resource-constrained environments. To overcome these limitations, researchers are actively exploring multiple strategies to enhance the efficiency and scalability of HE. Algorithmic optimizations, such as reducing bootstrapping overhead and leveraging approximate HE for specific use cases, are helping to improve computational performance. Additionally, hardware acceleration using Graphics Processing Units (GPUs), Field-Programmable Gate Arrays (FPGAs), and Application-Specific Integrated Circuits (ASICs) has shown promise in significantly reducing encryption and computation times.

Another crucial area of focus is standardization and integration with emerging technologies. Organizations such as NIST (National Institute of Standards and Technology) and leading technology firms are working on standardizing HE schemes, making them more accessible for widespread adoption. Furthermore, HE is being combined with technologies like secure multi-party computation (SMPC), differential privacy, and zero-knowledge proofs to enhance security while maintaining efficiency. Looking ahead, the future of HE will be shaped by advancements in quantum-resistant cryptography, secure artificial intelligence, and privacy-preserving cloud services. As more companies and institutions recognize the importance of data security in a digital economy, the demand for efficient HE implementations will continue to grow. With ongoing research in optimized cryptographic frameworks and hardware-driven acceleration, HE is expected to transition from a theoretical construct to a practical solution for real-world applications. In conclusion, while homomorphic encryption remains an evolving field, its potential for enabling secure, privacy-preserving computations is undeniable. With continuous improvements in efficiency, scalability, and hardware support, HE will play a pivotal role in shaping the future of secure data processing across industries.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Lagendijk, Reginald L., Zekeriya Erkin, and Mauro Barni. "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation." IEEE Signal Processing Magazine 30, no. 1 (2012): 82-105.

[2] Wang, Yongge, and Qutaibah M. Malluhi. "Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes." In European Symposium on Research in Computer Security, pp. 301-323. Cham: Springer International Publishing, 2016.

[3] Alabdulatif, Abdulatif, Heshan Kumarage, Ibrahim Khalil, and Xun Yi. "Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption." Journal of Computer and System Sciences 90 (2017): 28-45.

[4] Liu, Jibang, and Yung-Hsiang Lu. "Energy savings in privacy-preserving computation offloading with protection by homomorphic encryption." In Proceedings of the 2010 international conference on Power aware computing and systems, HotPower, vol. 10, pp. 1-7. 2010.

[5] Yonetani, Ryo, Vishnu Naresh Boddeti, Kris M. Kitani, and Yoichi Sato. "Privacy-preserving visual learning using doubly permuted homomorphic encryption." In Proceedings of the IEEE international conference on computer vision, pp. 2040-2050. 2017.