ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

Privacy-Preserving Data Sharing Using Homomorphic Encryption: A Review

[1]Akanksha Jain, [2]Monika Thakur, [3]Saleha Khan, [4]Dr. Prashant Sen
[12&3] Research Scholar, Department of Computer Science & Engineering,
Eklavya University, Damoh, Madhya Pradesh
[4]Associate Professor & Head, Department of Computer Science & Engineering,
Eklavya University, Damoh, Madhya Pradesh

Abstract

Data sharing is an essential aspect of modern digital applications, including healthcare, finance, cloud computing, and artificial intelligence. However, maintaining privacy and security during data exchanges presents significant challenges, especially with increasing concerns about data breaches and regulatory compliance. Homomorphic Encryption (HE) has emerged as a revolutionary cryptographic technique that allows computations to be performed on encrypted data without decryption, ensuring confidentiality throughout the processing phase. This review paper provides a comprehensive analysis of various HE schemes, including partially, somewhat, and fully homomorphic encryption. We discuss their applications in different domains, evaluate their security implications, and examine the computational challenges associated with their implementation. Additionally, we explore optimization strategies such as bootstrapping improvements, hybrid cryptographic models, and hardware acceleration techniques that aim to enhance HE's practicality. Real-world use cases in secure cloud computing, privacy-preserving machine learning, and secure multiparty computations are also discussed. Finally, we outline the challenges, potential solutions, and future research directions that will drive advancements in HE technology for secure and efficient data sharing.

Keywords: *Privacy-preserving, Homomorphic Encryption, Secure Data Sharing, Cloud Computing, Cryptography, Fully Homomorphic Encryption (FHE), Partially Homomorphic Encryption (PHE), Data Security.*

1. Introduction

Data privacy has become a critical issue in the modern digital landscape due to the increasing reliance on cloud computing, big data analytics, and artificial intelligence (AI). The growing number of cyber threats and stringent regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), have emphasized the need for robust data protection mechanisms (Kumar & Chaudhary, 2021). Traditional encryption techniques ensure data

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

confidentiality during storage and transmission but fail to protect data while it is being processed. This limitation creates security vulnerabilities, especially in cloud-based and multi-party computation scenarios (Zhang et al., 2020).

Homomorphic Encryption (HE) provides a novel cryptographic approach that allows computations to be performed on encrypted data without requiring decryption. The result of these computations, when decrypted, matches the outcome of operations performed on plaintext data (Gentry, 2009). This property makes HE a powerful tool for privacy-preserving data sharing, enabling secure outsourcing of computations to untrusted environments, such as cloud servers, without exposing sensitive information (Al-Riyami & Paterson, 2022).

The concept of HE dates back to the work of Rivest, Adleman, and Dertouzos (1978), who proposed partially homomorphic encryption (PHE) schemes capable of supporting either addition or multiplication operations on encrypted data. However, a major breakthrough occurred when Craig Gentry (2009) introduced the first fully homomorphic encryption (FHE) scheme, which allowed arbitrary computations on encrypted data through bootstrapping techniques. While Gentry's FHE scheme was revolutionary, it suffered from high computational overhead, limiting its practical adoption (Van Dijk et al., 2010).

Subsequent research has focused on optimizing HE for real-world applications. Somewhat homomorphic encryption (SHE) schemes, such as the Brakerski-Gentry-Vaikuntanathan (BGV) scheme (Brakerski et al., 2012) and the Cheon-Kim-Kim-Song (CKKS) scheme (Cheon et al., 2017), have improved efficiency while enabling limited-depth computations. Despite these advancements, HE still faces challenges related to computational cost, scalability, and key management (Hesamifard et al., 2017).

This paper presents a comprehensive review of HE techniques, their applications in various domains, and the challenges in their implementation. The subsequent sections discuss the mathematical foundations of HE, its role in privacy-preserving data sharing, and future research directions aimed at making HE more practical for real-world applications.

2. Literature Review

Several studies have explored the implementation and optimization of HE for secure data sharing.

- **Partially Homomorphic Encryption (PHE)**: Systems like RSA and ElGamal encryption support either addition or multiplication, but not both (Rivest et al., 1978).
- **Somewhat Homomorphic Encryption (SHE)**: Works by Boneh et al. (2005) introduced encryption schemes that allow limited homomorphic operations before requiring re-encryption.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

- **Fully Homomorphic Encryption (FHE)**: Gentry's (2009) breakthrough in FHE, utilizing bootstrapping techniques, has paved the way for practical applications, albeit with significant performance costs.
- **Optimization Techniques**: Subsequent research has focused on improving HE efficiency. The BGV scheme (Brakerski et al., 2012) and CKKS scheme (Cheon et al., 2017) optimize HE for integer and floating-point arithmetic, respectively.
- **Application Domains**: HE has been applied in privacy-preserving machine learning (Hesamifard et al., 2017), secure cloud computing (Lauter et al., 2015), and secure electronic voting systems (Damgård et al., 2010).

3. Mathematical Foundations and Key Properties of Homomorphic Encryption

3.1 Introduction to Homomorphic Encryption Mathematics

Homomorphic encryption relies on complex mathematical structures, primarily based on modular arithmetic, lattice-based cryptography, and algebraic number theory. The security of most HE schemes is derived from hard mathematical problems such as the Learning with Errors (LWE) problem, Ring-LWE (RLWE), and Integer Factorization (Gentry, 2009; Brakerski et al., 2014). These problems ensure that encrypted data remains secure against known cryptographic attacks while enabling computations to be performed directly on ciphertexts.

3.2 Algebraic Structures in Homomorphic Encryption

- **Modular Arithmetic:** HE schemes use modular arithmetic operations to maintain encrypted computations (Rivest et al., 1978). Given a plaintext message , an encryption function maps it to a ciphertext , which supports additive and multiplicative operations modulo some large integer .
- **Lattice-Based Cryptography:** Most FHE schemes leverage lattices due to their resistance to quantum attacks (Peikert, 2016). The hardness of solving LWE and RLWE problems ensures the security of homomorphic schemes.
- **Polynomial Rings and Fields:** Advanced HE schemes, such as the BGV and FV schemes, operate on polynomials over finite fields to enable efficient computations (Brakerski et al., 2014).

3.3 Key Properties of Homomorphic Encryption

Homomorphic encryption schemes must satisfy specific properties to enable secure computations on encrypted data:

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

- **Additive Homomorphism:** Given two encrypted values and , an HE scheme supports addition if: RSA and Paillier cryptosystems are examples of additively homomorphic encryption schemes (Paillier, 1999).
- **Multiplicative Homomorphism:** A scheme supports multiplication if:
  The ElGamal cryptosystem and RSA support multiplicative homomorphism (ElGamal, 1985).
- **Fully Homomorphic Encryption (FHE):** A system that supports both addition and multiplication over ciphertexts is called Fully Homomorphic Encryption (Gentry, 2009).

3.4 Homomorphic Encryption Schemes and Their Mathematical Frameworks

- **Partial Homomorphic Encryption (PHE):** Supports only one operation (addition or multiplication). Examples: RSA (multiplicative), Paillier (additive) (Paillier, 1999).
- **Somewhat Homomorphic Encryption (SHE):** Supports limited addition and multiplication operations before requiring decryption (Brakerski et al., 2011).
- **Fully Homomorphic Encryption (FHE):** Supports unlimited computations by leveraging bootstrapping techniques (Gentry, 2009).

3.5 Bootstrapping and Noise Management in HE

One of the main challenges in HE is ciphertext growth and computational noise accumulation. Bootstrapping, introduced by Gentry (2009), is a technique used to refresh ciphertexts and remove noise, allowing unlimited computations. Recent optimizations, such as modulus switching and key-switching techniques, improve the efficiency of bootstrapping in modern FHE schemes (Cheon et al., 2017).

3.6 Security Assumptions in Homomorphic Encryption

The security of HE is based on well-established cryptographic hardness assumptions:

- **Learning with Errors (LWE):** Hard to solve in polynomial time, making HE schemes resistant to brute-force attacks (Regev, 2005).
- **Ring-LWE (RLWE):** Extends LWE to polynomial rings for efficient key generation and encryption (Lyubashevsky et al., 2013).
- **Integer Factorization:** Used in classical cryptosystems like RSA (Rivest et al., 1978).

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

3.7 Challenges

Mathematical foundations such as modular arithmetic, polynomial rings, and lattice-based cryptography form the backbone of homomorphic encryption. While FHE schemes offer powerful capabilities, they remain computationally expensive. Future research aims to optimize efficiency by reducing noise accumulation and improving bootstrapping techniques.

4. Applications of HE in Privacy-Preserving Data Sharing

1. **Healthcare**: Secure genomic data analysis and privacy-preserving electronic health records (Lauter et al., 2014).
2. **Finance**: Secure multi-party computation for fraud detection and privacy-preserving banking transactions (Valdez et al., 2019).
3. **Cloud Computing**: Secure delegation of computations to untrusted cloud servers (Kamara & Lauter, 2010).
4. **Machine Learning**: Training encrypted models without exposing sensitive data (Hesamifard et al., 2017).

5. Challenges and Future Directions

Despite its potential, homomorphic encryption faces several challenges:

- **Computational Overhead**: FHE is significantly slower than traditional encryption schemes.
- **Key Management**: Ensuring secure key distribution in multi-party scenarios remains complex.
- **Scalability**: Applying HE to large-scale data remains impractical due to high computational requirements.
- **Hybrid Approaches**: Combining HE with secure multi-party computation (MPC) and differential privacy to enhance efficiency and security.

Future research should focus on optimizing HE efficiency, reducing bootstrapping costs, and integrating HE with emerging cryptographic techniques such as quantum-resistant encryption.

6. Conclusion

Homomorphic Encryption represents a transformative approach to privacy-preserving data sharing, enabling computations on encrypted data without compromising security. While its computational

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

overhead remains a major limitation, ongoing research in algorithmic optimization and hardware acceleration promises to make HE more practical. Future advancements in HE are expected to revolutionize secure computing, enabling privacy-preserving applications across various industries. Despite advancements, HE still faces practical challenges in scalability, efficiency, and usability. Future research must focus on optimizing computational complexity and integrating HE with complementary privacy-preserving techniques.

References

1. Boneh, D., Goh, E. J., & Nissim, K. (2005). Evaluating 2-DNF Formulas on Ciphertexts. Theory of Cryptography Conference (TCC).
2. Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2012). (Leveled) Fully Homomorphic Encryption without Bootstrapping. ITCS.
3. Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic Encryption for Arithmetic of Approximate Numbers. ASIACRYPT.
4. Damgård, I., Jurik, M., & Nielsen, J. B. (2010). A Generalization of Paillier's Public-Key System with Applications to Electronic Voting. International Journal of Information Security.
5. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. STOC.
6. Hesamifard, E., Ghassemi, F., Takabi, H., & Jones, C. (2017). Privacy-Preserving Machine Learning as a Service. PETS.
7. Kamara, S., & Lauter, K. (2010). Cryptographic Cloud Storage. Financial Cryptography and Data Security.
8. Lauter, K., Naehrig, M., & Vaikuntanathan, V. (2015). Can Homomorphic Encryption Be Practical? CCS.
9. Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On Data Banks and Privacy Homomorphisms. Foundations of Secure Computation.
10. Valdez, R., Agarwal, P., & Samanthula, B. K. (2019). Privacy-Preserving Financial Transactions using HE. Financial Cryptography and Data Security.
11. Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). Fully homomorphic encryption without bootstrapping. *SIAM Journal on Computing*.
12. Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. *ASIACRYPT*.
13. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st ACM Symposium on Theory of Computing*.
14. Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers*.