MDPI

Article

Review of Homomorphic Encryption Techniques for Secure Data Processing in Cloud-Based Healthcare Systems

Gideon Adjei[1,‡], Japheth Selorm HLORDJIE [2,‡], Konadu Zipporah Britwum[3,‡], Richard OTENG [4,‡], Ruth Fosuhemaa OWUSU [5,‡], David AWITOR [6,‡] and Philip Kwaku AMOABENG-MANU [7,]

[1] Affiliation 1; gideonad4@gmail.com
[2] Affiliation 2; japhethselorm@gmail.com
[3] Affiliation 3; zipporahbritwum@gmail.com
[†] Current address: Affiliation.
[‡] These authors contributed equally to this work.

Abstract: The paper reviews homomorphic encryption techniques to secure data in cloud-based healthcare systems. Through the use of secure computations on encrypted data, it is possible to ensure consistent patient confidentiality and to comply with health regulations. The study reviews the various types of homomorphic encryption and presents their present and potential future uses in healthcare, such as secure electronic health records and privacy-preserving data analysis. Furthermore, the paper highlights the potential of the technology in the areas of health data security and privacy-preserving data analytics. Nevertheless, challenges such as excessive computing power will have to be addressed to achieve wider acceptance.

Keywords: Homomorphic; Healthcare; Cloud; Encryption; Secure; Techniques; Patial; Somewhat

0. Introduction

The healthcare sector has witnessed significant changes over the last decade with the adoption of cloud-based services. Patient information technology in particular has experienced remarkable advancement. While such changes are beneficial as they heighten efforts toward modern efficiency, they create more and more burning issues respecting the confidentiality and security of information. It is obvious that medical information is highly sensitive implying that healthcare institutions have an obligation as much as it is technical – it is also legal to keep the information private, especially with information under health policies such as 'HIPAA'.

Homomorphic Encryption has developed and made itself very useful in the society, in such a way that computations are done tamper proof on gathered data. The implications of this feature endorse header encryption to the end this is well made, able to enhance privacy in usage of health care services based in cloud systems. However each of the 3 ranges of encryption homomorphic encryption is: partially homographic encryption,powerful homographic encryption and fully homomorphic encryption presents tradeoffs in efficiency and security thus appropriate for a specific use within healthcare.

This research analyzes the numerous techniques of invalid encryption in order to evaluate the possibilities of using these systems in cloud computing for processing healthcare information. More precisely, this analysis addresses the following questions: What are the advantages and disadvantages of various homomorphic encryption schemes? How do people adhere to healthcare rules in this domain? And what are the existing and future prospects of using HE in the analytics of big healthcare data?

In order to support such queries, qualitative research methodology was used and all relevant information concerning the topic was obtained from literature review. The findings from this research will be useful in determining the various ways through which homomorphic encryption can be implemented for improved security and integrity of

Citation: Adjei, G.; ,HLORDJIE J.S.; OWUSU, R.S. Review of Homomorphic Encryption Techniques for Secure Data Processing in Cloud-Based Healthcare Systems. *Journal Not Specified* **2024**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

healthcare information systems over the cloud and hence safer healthcare delivery services in the modern world.

This example provides a clear overview of the research topic, highlights the significance of using homomorphic encryption in healthcare and leads to the systematic review that is presented subsequently.

0.1. Significance

The value of this investigation is because it provides detailed information and assessment of those homomorphic encryption techniques with respect to their practical applications to healthcare based cloud technologies. As the scope of this study aims to assess the advantages and disadvantages of every single method, it is aimed at contributing the working solution towards the problem of information protection in the area of medicines and healthcare, such that important data concerning patients are kept safe and sound, while the enriched data processing and analysis are ongoing. This research makes sense particularly when health care institutions move more towards the utilization of cloud services and it becomes necessary to incorporate encryption solutions that satisfy legislative requirements and align with the emerging technologies in the sector.

As such, this research not only provides solutions to contemporary security problems within implementations of secure processing of health data but also extends the frontiers of progress in secure health data processing making the research beneficial to both health care professionals and technology experts.

1. Literature Review

1.1. Review of Related Works

Healthcare systems as it failed to address the necessity for real-time data processing in clinical settings. This limitation made it difficult to understand how these techniques can be applied to protecting patient's sensitive health information.

Unlike earlier works that have restricted themselves on that particular aspect of HE in various sectors including education and finance, Zhang et al. (2021)[20] reviewed instances where HE has been successfully deployed in healthcare systems among other fields. An important paper was authored by Zhang et al. (2021), which synthesized a broad spectrum of homomorphic encryption approaches comprehensively besides their theoretical underpinnings and potential uses. Even though this study has provided crucial insight about HE's technicality without going beyond general data security solutions, there remains scant information regarding health specific implications particularly because healthcare regulations impose unique challenges and there is always need for timely access to medical information at hospitals' emergency centers.

These include Gupta et al's (2020)[21] analysis that highlighted how different schemes were useful in terms of speed and size; however such factors are not sufficient for deeper discussion on how they relate directly to patient records confidentiality issues encountered during the transmission phase.

The issue of data protection and privacy in hospitals is not new. It has been with us since time immemorial; however, its importance cannot be understated in recent years as most medical data are now stored on the cloud and accessed remotely for better service delivery purposes (Zhang, 2021). In this regard, there has been a significant increase in review studies that focus on cryptographic techniques especially homomorphic encryption. In addition to addressing key points relating to different homomorphic encryption techniques, one of the most all-encompassing reviews is done by Zhang et al. (2021). The theoretical basis of HE is emphasized along with its possible uses across multiple industries including healthcare. Nevertheless, healthcare specific applications are only lightly touched upon in this review while general data security aspects are mainly discussed without getting deep into issues like strict healthcare regulations and real time data processing requirements within hospital settings. There has been a lot of reviews that have also written about homomorphic encryption in cloud computing (Gupta et al, 2020). The authors emphasized

that different HE schemes could be very efficient and scalable depending on the way they operate. Nonetheless, while it addressed computational efficiency in cloud environments heavily it did not consider how this remains important when looking at healthcare systems because instantaneous response is always required.

2. Methodology

2.1. Introduction

This section discusses the method and procedures used to arrive at the answers in this research. This section will cover the research design, paper analysis and selection techniques, and reasons for choosing a particular method

2.2. Research Design

This research provides mainly a review and comparative analysis on Homomorphic Encryption Techniques for Secure Data Processing in Cloud-Based Healthcare Systems.

2.3. Scope

This research seeks to answer the following research questions:

1. What is Homomorphic encryption? Red
2. How do different homomorphic encryption techniques (PHE, SWHE, FHE) compare in terms of efficiency and security for healthcare data processing in cloud environments? Blue
3. How does homomorphic encryption ensure patient data privacy and compliance with healthcare regulations? Yellow
4. What are the current and potential future applications of homomorphic in healthcare data analytics? Green

These questions aim at exploring the various techniques implemented in the classes of homomorphic encryption techniques for healthcare applications. Their benefits, techniques and challenges are explored and compared with one another.

2.4. Approach

In this research a qualitative approach was adopted aimed at understanding the theoretical implications of the various techniques of HE and evaluation of their practical applications in healthcare. Data collection This section explains the systematic procedure that was followed to gather qualitative data on the research question. From the recommended research databases or sources, the following databases were used in the research:

1. Science Direct
2. Google Scholar
3. IEEE Xplore

The databases given above is in the order of the most used databases in the research. Research key terms was determined from the given research topic. The key terms are given as follows: Homomorphic Encryption Techniques Secure data processing Cloud-based healthcare From the key terms, a research string was designed to help in querying the selected databases.

2.4.1. Search string

(“Homomorphic Encryption” OR “secure data processing” OR “processing encrypted data”) AND (“Techniques “) AND (“cloud-based” OR “cloud” OR “cloud environment”) AND (“healthcare” OR “health”)

Result From Query After making the queries, the results were observed and recorded accordingly without any filtering. The papers were sorted based on their relevance to the search string. After recording, “since 2020” filtering was applied to get the most current papers(in a span of last 4 years). The search results is summarized in the table given below:

Table 1. This is a table caption.

Filter	Science Direct	Google Scholar	IEEE Xplore
Without filter	1,173	N/A	1049
With filter (4 years span)	720	N/A	811

2.5. Data Analysis

The analysis was done by evaluating the:

1. Benefits
2. Technique
3. Challenges

of various HE techniques. The benefits and challenges are analyzed together in terms of their:

- Efficiency
- Security
- Applicability in healthcare
- Compliance with regulations

Techniques are discussed and compared separately.

2.5.1. Review Tables

At the end of each discussion of various techniques, a summary table is used to better compare each technique or scheme of HE and its application in healthcare systems. The tables provide a visual demonstration of the strengths and weaknesses of the various techniques.

2.6. Thematic Analysis

Initially, the abstract of the paper is read to verify the paper is relevant to the research topic. During reading of the article, the ideas are fragmented by highlighting the relevant ideas with color codes based on each research question. The coded fragments are then pieced together and trends are studied to make analysis to arrive at a conclusion. This was achieved by leveraging the use realtime editing tools (google docs specifically) to allow collaboration among the research team. Validation of Findings Cross-verification By reviewing at least 15 research papers, and picking information and cross checking from different articles ensured that our findings were consistent and reliable. Limitations: Our research was only based on secondary data. No direct approach was used to obtain our own results and conclusions, thus it depends on publicly available articles.

Ethical considerations We ensured that each paper reviewed was correctly cited, referenced and fairly represented to ensure data integrity.

This is an example of a quote.

3. Actual Review

3.1. What is Homomorphic Encryption?

Homomorphic encryption (HE) is a form of encryption that allows computations to be performed directly on encrypted data, producing an encrypted result that, when decrypted, matches the result of operations performed on the plaintext. This unique property enables secure data processing in environments where data privacy is paramount, such as in cloud computing and healthcare.

3.1.1. Types of Homomorphic Encryption

1. Partially Homomorphic Encryption (PHE):
    - Supports either addition or multiplication, but not both.

- Examples include the RSA encryption system (which supports multiplicative operations) and the Paillier encryption system (which supports additive operations).
- PHE is limited in its applicability due to the restriction to a single type of operation[8][6].

2. Somewhat Homomorphic Encryption (SWHE):
   - Supports both addition and multiplication, but only for a limited number of operations before the ciphertext becomes too noisy to decrypt properly.
   - SWHE offers a middle ground between PHE and FHE, providing more flexibility at the cost of increased complexity[8].
3. Fully Homomorphic Encryption (FHE):
   - Supports an unlimited number of both addition and multiplication operations.
   - FHE is the most powerful type of homomorphic encryption, allowing any computable function to be applied to encrypted data.
   - Despite its theoretical advantages, FHE remains computationally expensive and is less practical for real-time applications due to its high overhead[8][1][6].

Homomorphic encryption is crucial for maintaining data privacy in cloud computing, where sensitive information can be processed without exposing it to potential security threats. This capability is particularly important in sectors like healthcare, where patient confidentiality is a legal and ethical requirement.

Table 2. Summary of Types of Homomorphic Encryption

Type of Homomorphic Encryption	Description	Operations Supported	Example
Partially Homomorphic Encryption (PHE)	Supports a single type of operation (either addition or multiplication) on encrypted data.	Addition OR Multiplication	RSA, Paillier
Somewhat Homomorphic Encryption (SWHE)	Supports both addition and multiplication, but only for a limited number of operations.	Limited Addition and Multiplication	BGV
Fully Homomorphic Encryption (FHE)	Supports unlimited addition and multiplication operations on encrypted data.	Unlimited Addition and Multiplication	Gentry's FHE

3.2. How do different homomorphic encryption schemes (PHE, SWHE, FHE) compare in terms of efficiency and security for healthcare data processing in cloud environments?

This section discusses the benefits, challenges and techniques.

3.2.1. Efficiency:

1. PHE (Partially Homomorphic Encryption):
   - Efficiency: Highly efficient for operations it supports (either addition or multiplication), making it suitable for specific tasks like secure voting or simple data aggregation.
   - Limitations: The inability to perform both types of operations restricts its application in more complex data processing tasks, such as those required in healthcare[8].

2. SWHE (Somewhat Homomorphic Encryption):
    - Efficiency: Offers a balance between operational flexibility and computational efficiency. SWHE can handle a limited number of both addition and multiplication operations, making it more versatile than PHE.
    - Limitations: The noise introduced with each operation limits the number of operations that can be performed, which can be a drawback in healthcare scenarios requiring extensive data processing[8].
3. FHE (Fully Homomorphic Encryption):
    - Efficiency: FHE is computationally intensive and requires significant processing power, making it less practical for real-time healthcare applications. The high computational overhead can lead to delays, which is critical in environments like healthcare where timely access to data is essential.
    - Advantages: FHE's ability to perform unlimited operations without decryption makes it the most secure and flexible option, ideal for applications where comprehensive data processing is needed without compromising privacy[8][1].

3.2.2. Security:

1. PHE: While secure for the operations it supports, PHE's limited functionality can make it less secure in environments where multiple types of operations are needed. Its simplicity, however, reduces the attack surface compared to more complex schemes[8].
2. SWHE: Provides better security than PHE by supporting both addition and multiplication, albeit in a limited capacity. The noise accumulation poses a security risk if not managed properly, as it can lead to decryption failures[8].
3. FHE: Offers the highest level of security by supporting any computable function on encrypted data. However, the complexity of FHE also introduces potential vulnerabilities, especially in implementation. Despite this, FHE is the preferred choice for applications requiring the utmost data privacy, such as in healthcare[8][1].

3.2.3. Techniques

PHE

- RSA Encryption
- Operation Supported: Multiplication.
- Mathematical Foundation: Based on the difficulty of factoring large integers, RSA can perform multiplicative homomorphic operations. Specifically, given two ciphertexts $c_1 = E(m_1)$ and $c_2 = E(m_2)$, their product $c_1 \times c_2$ decrypts to $m_1 \times m_2$.
- Key Idea: The multiplicative property allows one to multiply ciphertexts to obtain a new ciphertext that encrypts the product of the plaintexts.
- **Paillier Encryption:**
- Operation Supported: Addition.
- Mathematical Foundation: Based on the composite residuosity problem, the Paillier cryptosystem allows for additive homomorphic operations. Given two ciphertexts $c_1 = E(m_1)$ and $c_2 = E(m_2)$, their product $c_1 \times c_2$ decrypts to $m_1 + m_2$.

Key Idea: The addition of encrypted values corresponds to the addition of plaintexts. This is particularly useful for applications like secure voting and privacy-preserving data aggregation.

SWHE

BGV Scheme (Brakerski-Gentry-Vaikuntanathan):

- Operations Supported: Limited addition and multiplication.
- Mathematical Foundation: Based on the Learning With Errors (LWE) problem or its ring variant (RLWE), the BGV scheme is designed to manage noise growth through techniques like modulus switching and key switching.

- Key Idea: By controlling noise growth, BGV allows for a certain number of addition and multiplication operations. It also introduces techniques to reduce the noise at the cost of increased computational complexity.
- LTV Scheme (Lopez-Alt, Tromer, and Vaikuntanathan):
- Operations Supported: Limited addition and multiplication.
- Mathematical Foundation: Similar to BGV, the LTV scheme is based on the RLWE problem but focuses on batch processing of operations, which improves efficiency.
- Key Idea: Supports a larger number of operations by batching several computations together, which helps in reducing the overhead of each operation.

FHE

1. Gentry's FHE Scheme:
   - Operations Supported: Unlimited addition and multiplication.
   - Mathematical Foundation: The original scheme by Craig Gentry introduced the concept of bootstrapping, which refreshes the ciphertext to reduce noise and allow for further operations.
   - Key Idea: Bootstrapping involves homomorphically evaluating the decryption circuit to reduce noise, effectively resetting the ciphertext and enabling additional operations.
2. CKKS Scheme (Cheon-Kim-Kim-Song):
   - Operations Supported: Unlimited addition and multiplication, optimized for approximate arithmetic.
   - Mathematical Foundation: Based on RLWE, the CKKS scheme is particularly suited for applications that tolerate small errors, such as machine learning on encrypted data.
   - Key Idea: CKKS supports efficient homomorphic operations on approximate values, which is useful for real-world applications that do not require exact precision.
3. BFV Scheme (Brakerski-Fan-Vercauteren):
   - Operations Supported: Unlimited addition and multiplication.
   - Mathematical Foundation: Also based on RLWE, the BFV scheme is designed for exact arithmetic and is often used in secure computation and privacy-preserving analytics.
   - Key Idea: BFV manages noise through a combination of modulus switching and relinearization techniques, making it possible to perform many operations without exceeding noise limits.

Table 3. This is a table caption.

Scheme	Efficiency	Security	Applicability in Healthcare	Challenges
PHE	High efficiency for specific tasks. Limited to a single operation type.	Secure for limited operations. Lower complexity reduces attack surface.	Simple data aggregation and voting.	Cannot perform both addition and multiplication.
SWHE	Balanced efficiency and operational flexibility. Can perform limited addition and multiplication.	More secure than PHE but vulnerable to noise accumulation.	Suitable for controlled environments like secure data analytics.	Limited number of operations before noise overwhelms the ciphertext.
FHE	Computationally intensive. High overhead costs.	Most secure; supports arbitrary computations on encrypted data.	Ideal for comprehensive data processing where privacy is critical (e.g., patient diagnostics).	High computational demand limits real-time applications

Table 4. Summary of Various Techniques

Type	Scheme	Operations Supported	Mathematical Foundation	Key Techniques
PHE	RSA	Multiplication	Integer Factorization	Multiplicative property
	Paillier	Addition	Composite Residuosity Problem	Additive property
SWHE	BGV	Limited Addition & Multiplication	LWE / RLWE	Modulus Switching, Key Switching
	LTV	Limited Addition & Multiplication	RLWE	Batching operations
FHE	Gentry's Scheme	Unlimited Addition & Multiplication	Ideal Lattices, Bootstrapping	Bootstrapping
	CKKS	Unlimited Addition & Multiplication	RLWE (Approximate Arithmetic)	Approximate arithmetic, Noise management
	BFV	Unlimited Addition & Multiplication	RLWE	Exact arithmetic, Modulus switching

3.3. Enhancement of FHE For Healthcare applications

The research paper, titled "Privacy Preserving via Multi-Key Homomorphic Encryption in Cloud Computing," [2] proposes an advanced cryptographic approach to improve the privacy and efficiency of cloud computing in multi-user environments. The key findings and contributions are summarized as follows: The DGHV (Dijk, Gentry, Halevi, Vaikuntanathan) scheme is an important fully homomorphic encryption (FHE) scheme that builds on earlier theoretical foundations laid by Craig Gentry, who introduced the first practical

FHE scheme in 2009. The DGHV scheme offers a simpler and more understandable construction compared to Gentry's original scheme, making it a significant step forward in the development of FHE.

3.3.1. Enhancement of the DGHV Homomorphic Encryption Scheme:

Builds on the existing DGHV (Dijk, Gentry, Halevi, Vaikuntanathan) homomorphic encryption scheme by introducing modifications that remove limitations related to the parity of the ciphertext modulus. This innovation improves the scheme's noise management capabilities and ensures reliable decryption, even when multiple users are involved. The modified DGHV scheme serves as the foundation for the new multi-key homomorphic encryption (MKHE) approach Development of a Novel Multi-Key Homomorphic Encryption (MKHE) Scheme: The authors propose a new MKHE scheme that allows encrypted data from different users (each with their own encryption key) to be processed homomorphically. This means that operations can be performed on the encrypted data without needing to decrypt it first, ensuring that privacy is maintained throughout the process. The results of these operations can then be decrypted using a jointly computed secret key, enabling collaborative data processing without compromising individual user security.

3.3.2. Security and Efficiency Validation:

The security of the proposed MKHE scheme is rigorously analyzed. It is shown to be semantically secure under the assumption of the hardness of the approximate greatest common divisor (GCD) problem and the difficulty of factoring large integers. The scheme is also designed to be computationally efficient, making it practical for real-world cloud computing applications. The authors provide detailed proofs and discussions on the security assumptions and the potential impact of various attack vectors.

3.3.3. Experimental Evaluation:

Through a series of simulations, the authors demonstrate that the proposed MKHE scheme is computationally efficient, featuring reduced public key sizes and effective ciphertext noise management. These factors contribute to its suitability for real-time applications, where low latency and high throughput are critical. The paper includes detailed performance metrics, comparing the scheme's efficiency in different cloud computing scenarios. Comparative Analysis with Existing MKHE Schemes: The paper compares the proposed MKHE scheme with existing schemes, such as those based on NTRU and the GSW (Gentry-Sahai-Waters) framework. The proposed scheme is shown to have significant advantages, including simpler key management, reduced computational overhead, and a lower dependency on relinearization processes, which are often required in other homomorphic encryption techniques.

3.3.4. Critical Importance of Secure Data Processing:

The enhanced DGHV-based MKHE scheme is particularly relevant to cloud-based healthcare systems where multi-user collaboration is common. In such settings, multiple stakeholders (doctors, patients, healthcare providers) may need to perform operations on sensitive data, such as medical records, without exposing this data to unauthorized parties. The MKHE scheme ensures that these operations can be performed securely, preserving the confidentiality of patient data.

3.3.5. Suitability for Healthcare Applications:

The proposed scheme's ability to handle homomorphic operations across encrypted data from different users is highly applicable in healthcare scenarios. For instance, it could be used to securely aggregate patient data for research purposes, compute diagnostics across multiple encrypted datasets, or share information between healthcare providers without compromising patient privacy. The scheme's design, which minimizes noise and

maintains efficient decryption, is essential for the high standards required in medical data processing.

3.3.6. Performance Optimization in Healthcare Systems:

Performance is a key concern in healthcare, where real-time data processing can be a matter of life and death. The paper's focus on reducing computational overhead and improving the management of ciphertext noise directly addresses these concerns. This makes the scheme suitable for applications requiring rapid processing, such as emergency response systems, telemedicine platforms, and cloud-based diagnostic tools.

3.3.7. Comparative Strengths and Considerations:

The comparative analysis provided in the paper is invaluable for your research project. It offers a clear understanding of how the proposed MKHE scheme stacks up against other techniques, such as those based on lattice-based cryptography (NTRU) or the GSW framework. This analysis will help in determining the best encryption technique for specific cloud-based healthcare applications, considering factors like key management complexity, computational efficiency, and security guarantees.

3.3.8. Direction for Future Research:

MKHE schemes for even larger datasets, improving the efficiency of multi-party computations in healthcare, and exploring hybrid encryption models that could offer even stronger security or performance benefits. These directions could be critical for advancing the state-of-the-art in secure data processing within cloud-based healthcare systems [2]

Table 5. Summary Table for Multi-Key Homomorphic Encryption (MKHE)

Aspect	Description
Multi-Key Support	Allows multiple users, each with their own encryption keys, to perform joint computations on encrypted data.
Security	Ensures that combined operations on ciphertexts remain secure, maintaining the privacy of each user's data.
Key Management	Involves complex key management, including joint decryption processes to ensure that no single key or plaintext is exposed during computations.
Applications	Collaborative data processing, privacy-preserving machine learning, multi-tenant cloud services.
Challenges	Efficiency, key management complexity, scalability issues with increasing number of participants.
Examples of MKHE Schemes	NTRU-based MKHE, GSW framework-based MKHE, DGHV-based MKHE.

3.4. How does homomorphic encryption ensure patient data privacy and compliance with healthcare regulations?

Homomorphic encryption ensures patient data privacy by enabling data processing in an encrypted state, thereby protecting sensitive information throughout its lifecycle. This is particularly important in healthcare, where regulations like the Health Insurance Portability and Accountability Act (HIPAA) mandate strict controls on patient data.

3.4.1. Key Points:

- Encryption During Processing: Homomorphic encryption allows healthcare providers to perform operations on encrypted data without exposing the underlying information, ensuring that patient data remains private even during analysis and processing[1].
- Regulatory Compliance: By keeping data encrypted, HE helps healthcare organizations comply with regulations that require the protection of patient information against unauthorized access and data breaches. This is essential for maintaining trust and ensuring that patient data is handled in a legally compliant manner[8].
- Secure Data Sharing: HE facilitates secure data sharing among healthcare providers, enabling collaborative analysis of patient data without compromising privacy. This is particularly useful in cloud environments, where data may be transmitted across different entities and systems [1].
-

Table 6. Homomorphic Encryption (HE) in Healthcare: Compliance and Challenges

Aspect	Description	How HE Ensures Compliance	Challenges
Data Privacy	Encrypts data so that computations can be performed without exposing sensitive information.	HE allows secure processing and sharing of patient data, ensuring that no plaintext data is exposed during operations.	Computational overhead and integration with existing healthcare systems.
Regulatory Compliance	Compliance with HIPAA and other healthcare regulations.	HE ensures that data remains encrypted throughout its lifecycle, meeting regulatory requirements for data protection.	Complexity of implementing HE in real-world systems and ensuring compatibility with other regulatory standards.
Secure Data Sharing	Facilitates secure sharing of encrypted data among healthcare providers.	Enables collaboration and data sharing without exposing underlying patient information.	Managing encryption keys and maintaining system efficiency.

3.5. What are the current and potential future applications of homomorphic encryption in healthcare data analytics?

3.5.1. Current Applications:

Secure Electronic Health Records (EHRs):Homomorphic encryption is used to secure EHRs stored in cloud environments. By encrypting patient data before storage, healthcare providers can ensure that sensitive information remains confidential while still being accessible for necessary medical operations[8][1]. HE allows healthcare providers to perform necessary computations on EHRs, such as aggregating data for research or clinical analysis, without exposing the data itself[8].

1. Privacy-Preserving Data Analytics:
   - HE enables the analysis of encrypted health data, allowing healthcare organizations to gain insights without risking data privacy. This is crucial for tasks like predictive analytics, where patient data is analyzed to forecast health outcomes[7].
   - Use cases include the secure analysis of medical imaging, genomic data, and other sensitive health information[7].

3.5.2. Future Applications:

2. Machine Learning on Encrypted Data:
   - Homomorphic encryption could enable the development of machine learning models that operate on encrypted datasets. This would allow healthcare providers to leverage advanced analytics and AI-driven insights while maintaining patient confidentiality[7].
   - For example, machine learning models could be trained on encrypted health records to predict disease outbreaks or to personalize treatment plans, all while ensuring that the underlying data remains secure[1].
   -
3. Public Health Applications:
   - In the context of public health, HE can be used to enable privacy-preserving contact tracing and epidemic monitoring. For instance, during the COVID-19 pandemic, homomorphic encryption was proposed as a method for securely determining close contacts and enforcing social distancing measures without compromising individual privacy[7].
   - Future applications could extend to secure sharing of epidemiological data across borders, enabling global cooperation in disease prevention and control while adhering to privacy regulations[7].
   -
4. Expansion in Cloud-Based Healthcare Services:
   - As cloud services become more integral to healthcare, HE will play a crucial role in ensuring the security of cloud-based healthcare applications. Future developments may include more efficient HE algorithms that can support real-time data processing and integration with emerging technologies like blockchain[7].
   - HE could also facilitate secure telemedicine services, where patient consultations and medical records are handled entirely in encrypted form, protecting patient privacy throughout the interaction[1].

Table 7. Summary of Future Applications of Homomorphic Encryption in Healthcare

Application	Description	Current Status	Future Potential
Electronic Health Records (EHRs)	Secure storage and processing of EHRs in cloud environments.	Widely used for securing sensitive patient data in cloud storage.	Expanded use in real-time data processing and analysis without compromising privacy.
Privacy-Preserving Data Analytics	Enables secure analytics on encrypted health data.	Used for privacy-preserving predictive analytics and research.	Integration with machine learning models to enhance predictive healthcare analytics.
Public Health Monitoring	Privacy-preserving contact tracing and epidemic monitoring.	Proposed for use in COVID-19 and other public health initiatives.	Broader adoption in global public health strategies, enabling secure data sharing across borders.
Machine Learning on Encrypted Data	Training and inference on encrypted datasets to protect patient privacy.	Emerging area of research with limited real-world implementation.	Potential to revolutionize personalized medicine and large-scale health data analysis.

4. Conclusion

Homomorphic encryption (HE) stands out as a critical technology in the ongoing effort to secure sensitive healthcare data in cloud-based systems. This review has explored the various types of homomorphic encryption—Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE)—and analyzed their applicability, efficiency, and security within the healthcare sector. While PHE and SWHE offer practical solutions for specific use cases, their limitations in supporting comprehensive data operations highlight the need for more robust approaches like FHE, despite its current computational challenges.

The review of existing literature revealed that while significant progress has been made in applying HE to healthcare, many studies have not fully addressed the unique challenges posed by healthcare regulations, the need for real-time processing, and the practical deployment of HE in large-scale cloud environments. This gap underscores the importance of targeted research that not only compares these encryption techniques in theory but also evaluates their real-world applicability and compliance with healthcare-specific requirements.

Looking forward, the continued development and optimization of HE techniques, particularly in enhancing the efficiency and reducing the computational overhead of FHE, will be crucial in enabling their widespread adoption in healthcare. Future research should focus on overcoming the practical barriers to implementation, such as integrating HE with existing healthcare systems, ensuring scalability, and maintaining compliance with evolving data protection regulations. By addressing these challenges, homomorphic encryption can become a cornerstone in the secure and efficient processing of healthcare data, ultimately leading to safer and more privacy-preserving healthcare services in the digital age.

References

1. Sammeta, Naresh, Parthiban, Latha, et al. (2021). *Medical data analytics for secure multi-party-primarily based cloud computing utilizing homomorphic encryption*. *Journal of Scientific & Industrial Research*, 80(08), 692–698.
2. Salim, Mikail Mohammed, Kim, Inyeung, Doniyor, Umarov, Lee, Changhoon, Park, Jong Hyuk (2021). *Homomorphic encryption based privacy-preservation for IoMT*. *Applied Sciences*, 11(18), 8757. MDPI.
3. Devi, P., Sathyalakshmi, S., Subramanian, D. Venkata (2020). *A comparative study on homomorphic encryption algorithms for data security in cloud environment*. *International Journal of Electrical Engineering & Technology*, 11(2), 129–138.
4. Syafalni, Infall, Fadhli, Hamdani, Utami, Wuri, Dharma, Gede Satya Adi, Mulyawan, Rahmat, Sutisna, Nana, Adiono, Trio (2020). *Cloud security implementation using homomorphic encryption*. In *2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 341–345. IEEE.
5. Kavitha, S., Pavithra, B. S., Shashikala, A. B., Jagadeesh, B. N., Mageswari, P. Uma, Marichi, Dileep (2024). *Preserve the Medical Data using Secure Partially Homomorphic Encryption with Blockchain Technology in Smart Healthcare*. In *2024 Second International Conference on Data Science and Information System (ICDSIS)*, 1–6. IEEE.
6. Marwan, Mbarek, Karti, Ali, Ouahmane, Hassan (2021). *Proposal for a secure data sharing and processing in cloud applications for healthcare domain*. *International Journal of Information Technology and Applied Sciences (IJITAS)*, 3(1), 10–17.
7. Alharbi, Ayman, Zamzami, Haneen, Samkri, Eman (2020). *Survey on homomorphic encryption and address of new trend*. *International Journal of Advanced Computer Science and Applications*, 11(7). Science and Information (SAI) Organization Limited.
8. Awadallah, Ruba, Samsudin, Azman (2020). *Homomorphic encryption for cloud computing and its challenges*. In *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 1–6. IEEE.
9. Roumpies, Fotios, Kakarountas, Athanasios (2023). *A Review of Homomorphic Encryption and its Contribution to the Sector of Health Services*. In *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, 237–242.

10. Saxena, Urvashi Rahul, Alam, Taj (2023). *Role-based access using partial homomorphic encryption for securing cloud data*. *International Journal of System Assurance Engineering and Management*, 14(3), 950–966. Springer.
11. Yulliwas Ameur, Samia Bouzefrane, and Le Vinh Thinh. Handling security issues by using homomorphic encryption in multi-cloud environment. *Procedia Computer Science*, 220:390–397, 2023. https://www.sciencedirect.com/science/article/pii/S1877050923005859.
12. Hiral S. Trivedi and Sankita J. Patel. Homomorphic cryptosystem-based secure data processing model for edge-assisted IoT healthcare systems. *Internet of Things*, 22:100693, 2023. https://www.sciencedirect.com/science/article/pii/S2542660523000161.
13. Daxin Huang, Qingqing Gan, Xiaoming Wang, Marek R. Ogiela, and Xu An Wang. Privacy preserving IoT-based crowd-sensing network with comparable homomorphic encryption and its application in combating COVID19. *Internet of Things*, 20:100625, 2022. https://www.sciencedirect.com/science/article/pii/S2542660522001068.
14. Xuelian Li, Hui Li, Juntao Gao, and Runsong Wang. Privacy preserving via multi-key homomorphic encryption in cloud computing. *Journal of Information Security and Applications*, 74:103463, 2023. https://www.sciencedirect.com/science/article/pii/S2214212623000479.
15. Min Zhao E and Yang Geng. Homomorphic Encryption Technology for Cloud Computing. *Procedia Computer Science*, 154:73–83, 2019. https://www.sciencedirect.com/science/article/pii/S1877050919307811.
16. Wang Ren, Xin Tong, Jing Du, Na Wang, Shan Cang Li, Geyong Min, Zhiwei Zhao, and Ali Kashif Bashir. Privacy-preserving using homomorphic encryption in Mobile IoT systems. *Computer Communications*, 165:105–111, 2021. https://www.sciencedirect.com/science/article/pii/S0140366420319708.
17. Qiong Liu, Feng Zhou, and Han Chen. Secure medical data on cloud storage via DNA homomorphic encryption technique. *Physical Communication*, 64:102295, 2024. https://www.sciencedirect.com/science/article/pii/S1874490724000132.
18. Mohanad A. Mohammed and Hala B. Abdul Wahab. Enhancing IoT Data Security with Lightweight Blockchain and Okamoto Uchiyama Homomorphic Encryption. *CMES - Computer Modeling in Engineering and Sciences*, 138(2):1731–1748, 2023. https://www.sciencedirect.com/science/article/pii/S1526149223000607.
19. Bo Wang, Hongtao Li, Yina Guo, and Jie Wang. PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Applied Soft Computing*, 146:110677, 2023. https://www.sciencedirect.com/science/article/pii/S1568494623006956.
20. Zhang, Wei, Li, Xin, Wang, Yue (2021). *Homomorphic encryption: Theoretical foundations and applications*. *Journal of Cryptographic Engineering*, 11(2), 123–145. Springer.
21. Gupta, Rajesh, Sharma, Priyanka (2020). *Homomorphic encryption in cloud computing: Efficiency and scalability*. *IEEE Access*, 8, 20032–20044. IEEE.
22. Alharbi, Mohammed, Ghanem, Amal (2022). *Privacy-preserving techniques in cloud-based healthcare: The role of homomorphic encryption*. *Computers & Security*, 113, 102565. Elsevier.