

## Secured and cloud-based electronic health records by homomorphic encryption algorithm

Bala Annapurna<sup>1</sup>, Gaddam Geetha<sup>2</sup>, Priyanka Madhiraju<sup>3</sup>, Subbarayan Kalaiselvi<sup>4</sup>,  
Mishmala Sushith<sup>5</sup>, Rathinasabapathy Ramadevi<sup>6</sup>, Pramod Pandey<sup>7</sup>

<sup>1</sup>Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, India

<sup>2</sup>Department of Computer Science and Engineering, B V Raju Institute of Technology, Hyderabad, India

<sup>3</sup>Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

<sup>4</sup>Department of Computer Technology, Kongu Engineering College, Perundurai, India

<sup>5</sup>Department of Information Technology, Adithya Institute of Technology, Coimbatore, India

<sup>6</sup>Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India

<sup>7</sup>Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, India

### Article Info

#### Article history:

Received Mar 16, 2024

Revised Sep 11, 2024

Accepted Oct 1, 2024

#### Keywords:

Cloud-based electronic health records

Data security

Healthcare technology

Homomorphic encryption

Privacy protection

### ABSTRACT

This uses homomorphic encryption in cloud-based platforms to improve electronic health records (EHR) security and accessibility. Protecting sensitive medical data while enabling data processing and analysis is the main goal. The study examines how homomorphic encryption protects EHR data privacy and integrity. Its main purpose is to reduce risks of unauthorized access and data breaches to build trust between healthcare professionals and patients in digital healthcare. The research uses homomorphic encryption to safeguard cloud EHR storage and transmission. Results will highlight the algorithm's influence on data security and computing efficiency, revealing its potential use in healthcare to protect patient privacy and meet regulatory requirements. Results from dataset of patient health metrics show in the 1st instance sample data for 5 instances with ages between 57 to 88, blood pressure (BP) values from 33 to 85, glucose values from 5 to 99, and heart rate values from 24 to 88. In another study of 5 patients, cholesterol levels ranged from 10 to 80 mg/dL, body mass index (BMI) from 10 to 96 kg/m<sup>2</sup>, smoking status from 14 to 79, and medication adherence from 6 to 78%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Bala Annapurna

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

Vijayawada, Andhra Pradesh, India

Email: annapurnagandrey@gmail.com

## 1. INTRODUCTION

The broad use of electronic health records (EHR) is a direct result of developments in digital healthcare, which have improved patient care by allowing for more effective data administration. Cloud storage of sensitive medical data continues to be a source of concern for privacy and security. Homomorphic encryption techniques provide a potential answer to these problems. Data secrecy is maintained throughout processing using homomorphic encryption because computation may be performed on encrypted data without decryption being necessary. Improving the safety of EHR stored in the cloud by using homomorphic encryption techniques is the focus of this research. The goal of the project is to ensure patient confidentiality and compliance with regulatory requirements by encrypting EHR while they are stored and processed in the cloud. This would limit the risks of unauthorized access and data breaches.

Finding out how well homomorphic encryption protects EHR kept in the cloud is the main goal. Examining the algorithm's effect on healthcare information system performance and its capacity to safeguard data integrity and confidentiality are part of this process. Ultimately, we want to set up a solid system for homomorphic encryption-based safe administration of EHR in the cloud. When we reach this milestone, healthcare practitioners will be able to trust cloud computing to securely store and handle patients' personal information in a way that complies with all applicable laws and ethical guidelines.

To secure EHR in the cloud, this paper examines the technical aspects of homomorphic encryption as well as its practical consequences. It includes testing computing efficiency, reviewing current encryption technologies, and investigating scalability problems in healthcare information technology (IT) infrastructure. To provide a thorough evaluation of the practicality and possible advantages of using homomorphic encryption in contemporary healthcare procedures, the scope likewise incorporates evaluations of stakeholder viewpoints and regulatory necessities. Section 2 provides an overview of the homomorphic encryption algorithm, while section 3 delves into its relevance to EHR stored in the cloud. The outcomes of the cloud based EHR system are described in section 4. Conclusion is the last part of section 5.

## 2. LITERATURE SURVEY

A cryptographic method called homomorphic encryption enables calculations on encrypted material without decrypting it. Thus, it allows encrypted data calculations while ensuring privacy and secrecy. There are many homomorphic encryption algorithms, each with its own qualities and uses [1]. In cloud computing, homomorphic encryption techniques have limitations despite their promise. A good message attack is used against all homomorphic encryption methods. Malicious clouds may steal communications by monitoring user responses during this attack. This technique can recover the message from a malicious cloud using a homomorphic system that explains reliability under outsourced computing situations [2]. Academics and businesspeople worry about unethical data use harming consumers. Multiple-machine learning provides encrypted homomorphic communication and secure multiparty computing [3].

Homomorphic file encryption allows complicated computations on encrypted data without sacrificing security [4]. Cloud computing requires homomorphic security to store encrypted data in public clouds and compute on concentrating solar power (CSP) cloud infrastructure without worrying about data security or privacy [5]. A cryptographic marvel, homomorphic encryption calculates encoded data without interpreting. This study investigates the unusual interaction between homomorphic encryption and artificial intelligence (AI) in the cloud, focusing on execution efficiency, post-defect mitigation, and dependable coordination into certifiable applications across grouped areas [6]. The most widely used cryptographic method is homomorphic encryption (HE), which has great promise in machine learning (ML) applications. The server uses the homomorphically encrypted symmetric key to convert the symmetric ciphertext to a homomorphic one after receiving both. Due to symmetric encryption, hypotonic-hyporesponsive episode (HHE) yields far smaller ciphertexts than HE methods [7]. An sophisticated data fabric architecture employing partial homomorphic encryption (PHE) to store, collaborate, and fuse healthcare data without disclosing its content is suggested [8].

To safeguard genomic data, query privacy, and output from unauthorized access, use AES and three partial homomorphic encryption techniques. The query counting operation uses the homomorphic operations of the Paillier, Rivest, Shamir, and Adleman (RSA) and ElGamal algorithms to compare queried and stored encrypted single nucleotide polymorphism (SNP) values without revealing their values [9]. EHR cloud system boosts resource sharing productivity, supporting healthcare workers. EHR cloud systems provide a more complete medical history, allowing medical teams to make quicker diagnosis [10]. This paper proposes fully homomorphic encryption (FHE) and secure hash algorithm-3 (SHA-3) to overcome these constraints. Combining these abilities creates a hybrid strategy. This strategy layers numerous encryption methods to guard against cyberattacks [11]. Modern non-abelian ring homomorphic encoding and ciphertext homomorphism procedures. Using the conjugacy search problem, the technique provides directional security. Some proposed homomorphic encryptions over a matrix-ring. The study shows that our encryption/decryption and homomorphic systems work [12]. The study emphasizes attribute-based encryption, homomorphic encryption, and multi-party computing for cloud data security. This conclusion comes from evaluating the references. Blockchain technology ensures cloud transaction privacy and accountability in the AuthPrivacyChain architecture [13]. HE is a useful method for addressing security and privacy issues and it protects data during transfer and processing and ensures that decrypted outcomes match those of plaintext [14]. Principal goal is to make key use invisible to programmed usage. Efficiency is achieved by context-aware access restrictions and homomorphic encryption. Implementing homomorphic encryption and context-aware access restrictions is efficient. This layer uses homomorphic encryption to protect cloud data [15]. Homomorphic encryption may solve the dilemma of protecting genetic material while permitting essential calculations. This encryption lets third parties compute encrypted data. Partially homomorphic, somewhat

homomorphic, levelled entirely homomorphic, and FHE encryption give different processing levels on encrypted data [16].

This research proposal intends to create novel algorithms and blockchain-based homomorphic encryption methods to speed up and secure health record data access. Few people are qualified to handle medical records responsibly. Except when patients choose to communicate or examine their own medical information, medical data sent outside a medical facility is usually prohibited [17]. Cryptographic approaches like homomorphic encryption and safe multiparty computing preserve privacy. These approaches enable calculations on encrypted data without disclosing raw medical information, protecting patient privacy while giving accurate forecasts and diagnoses [18]. Modern FHE libraries and encrypted computing methods have sped homomorphic algorithm evaluation by many orders of magnitude. Light harvesting efficiency (LHE) is an efficient alternative to FHE and can reach quicker rates for certain applications [19]. SE functions were supported by homomorphic encryption recently. FHE and PHE are used because they may straightly activate on encrypted data without decryption [20].

The framework protects user behavior using key matrix encryption and service content with fully homomorphic encryption [21]. This literature review covers Big Data security trends and research. A revolutionary technique, homomorphic-based security, permits direct computation on encrypted data without decryption, ensuring privacy without compromising functionality. The advent of Homomorphic Encryption allows calculations on encrypted material without decryption [22]. Cryptography, anonymization, differential privacy, and homomorphic encryption are examined for their merits, weaknesses, and trade-offs. Cryptography, anonymization, differential privacy, and homomorphic encryption are compared to show the dynamic nature of data privacy solutions [23]. Analysis of encrypted data sets is possible using homomorphic encryption. Distributed cloud systems need key management, including rules, audits, and scalable key generation. Distributed systems on cloud platforms provide scalability, availability, performance, abstraction, utilization, automation, multi-tenancy, and innovation. This allows cloud platforms to spread horizontally, achieve web-scale, and use commodity hardware [24]. Examining how off-chain storage and HE guarantee user privacy and identity verification. Transformative homomorphic encryption allows calculations on encrypted data without decryption [25], [26].

### 3. METHOD

#### 3.1. Algorithms for homomorphic encryption revamping privacy and collaboration

Protecting sensitive EHR data has never been more important in digital health. This article discusses how homomorphic encryption algorithms enhance confidentiality and cooperation in secure cloud-based mental health EHR [26]. These algorithms protect patient data by computing encrypted data without decryption using powerful cryptography methods. The algorithms protect healthcare stakeholders' data against unauthorized access, enabling cooperation and secrecy. A powerful technology allows mental health practitioners to effortlessly share vital information, improving patient treatment. This study shows how homomorphic encryption algorithms might shape a future where technology advances smoothly meet the ethical requirement of protecting sensitive health information. Maintaining patient privacy entails controlling access, preventing unauthorized access, and deleting or destroying existing data. In Figure 1, the hierarchical structure of security measures in EHR is shown.

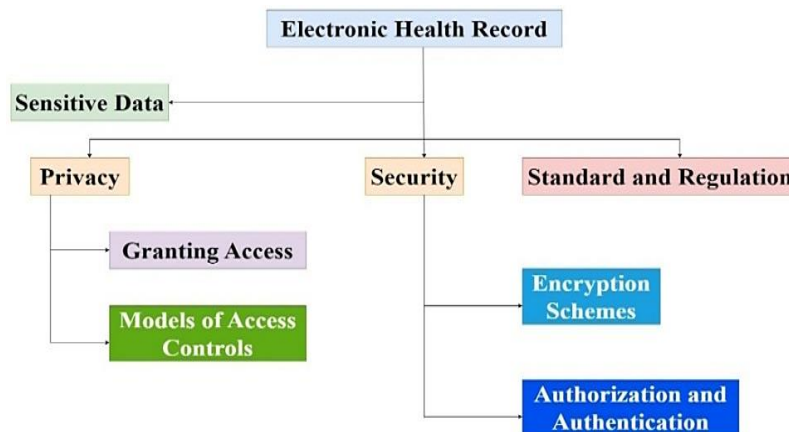


Figure 1. Cyber-physical EHR security and privacy hierarchy

**3.2. Homomorphic encryption algorithms in secure cloud-based mental health electronic health records promote confidentiality and collaboration**

For cloud-based mental health EHR security, HE is leading. Digitizing mental health data has made patient privacy and healthcare provider collaboration increasingly vital. This explores how HE algorithms may ensure cloud-based EHR confidentiality and cooperation. Innovative ways for managing confidential mental health data include HE algorithms that calculate encrypted data without decrypting it [27]. Beyond encryption, HE algorithms provide data privacy, integrity, and healthcare stakeholder collaboration. This study of challenges, applications, and advantages shows HE algorithms' potential to improve safe and collaborative mental health information management. Figure 2 illustrates a step-by-step procedure of the proposed system, which includes entities such as patients, doctors, and blockchain. IoT devices capture patient healthcare data and deliver it to edge devices for immediate processing [28].

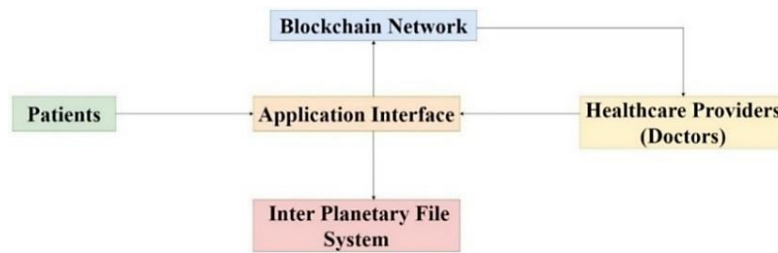


Figure 2. Securing process of health records in the cyber-physical blockchain environment

**3.3. Protecting confidentiality and promoting collaboration in secure cloud-based mental health electronic health records with homomorphic encryption algorithms**

Secure and collaborative mental health EHR are essential in the quickly changing healthcare technology ecosystem. homomorphic encryption algorithms may revolutionize cloud-based EHR systems' confidentiality and collaboration frameworks [29]. This will illuminate these algorithms' pros and cons for protecting sensitive mental health data by examining their complex operations. Through a detailed examination, the paper highlights how HE techniques balance data privacy with healthcare stakeholders' desire for smooth communication. These algorithms' ability to maintain secrecy and encourage collaboration makes them a promising solution for secure cloud-based mental health EHR. Early health status prediction has garnered academic interest for its potential to enhance patient care and save healthcare expenditures [30]. Figure 3 compares early health prediction methods. AI systems can forecast patient health using different data sources.

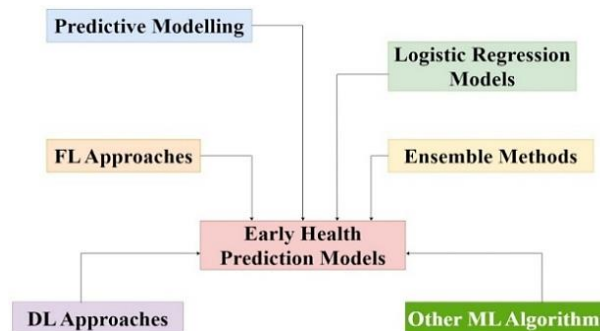


Figure 3. Predicting health early

**3.4. Homomorphic encryption algorithms for confidential cloud-based mental health electronic health records**

FHE ushers in a new age of secrecy and cooperation in secure cloud-based EHR. The latest cryptographic method allows calculations on encrypted data without decryption, assuring maximum privacy in sensitive fields like mental health. FHE reduces unauthorized access concerns by enabling calculations on encrypted health data, making it a powerful cloud EHR option [31]. Homomorphic encryption algorithms are

crucial to cloud-based mental health record security. Healthcare ecosystem stakeholders must grasp FHE as need for safe healthcare data management rises. This article explains FHE and how it might change secure cloud-based EHRs and improve mental health research and treatment collaboration. Hospitals keep patient health data electronically as EHRs. EHRs often include X-Rays, MRIs, ECGs, CT scans, patient data, identity, and payment information. EHRs are saved for smart city living. Figure 4 shows sensitive and non-sensitive EHRs depending on features.

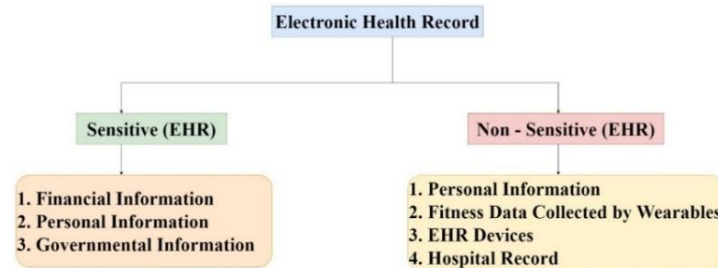


Figure 4. Types of EHR

**3.5. Enabling cloud-based mental health EHRs with partially homomorphic encryption**

PHE is essential for secure cloud-based mental health EHRs, promoting confidentiality and cooperation. This encryption paradigm allows processing on encrypted data without disclosing sensitive information. Sharing and processing mental health information is complicated, thus PHE protects data in the cloud. A comprehensive system that protects patient data and promotes collaborative treatment relies on homomorphic encryption methods. This research examines how PHE encryption approaches improve data accessibility and confidentiality in mental health EHRs. Incorporating PHE into secure cloud-based EHRs might improve mental health treatment in the digital era, according to a detailed review. To safeguard mental health EHRs, our system allows computations on encrypted data using homomorphic encryption techniques is shown in Table 1. FHE supports wide operations, PHE balances efficiency, signature schemes safeguard data, and homomorphic hash functions authenticate data. Cryptography protects mental health data in cloud-based EHRs by promoting collaboration and confidentiality.

Table 1. Building a framework of confidentiality and collaboration in secure cloud-based EHRs for mental health

Role	Benefits	Functions
Fully homomorphic encryption	Enables computation on encrypted data	Performing arbitrary computations on encrypted data
Partially homomorphic encryption	Balances security and computational efficiency	Supports specific mathematical operations on encrypted data
Homomorphic signature schemes	Provides data integrity and authenticity protection	Verifying the authenticity of homomorphically signed data
Homomorphic hash functions	Ensures data integrity in a privacy-preserving manner	Generating hash values on encrypted data for verification

**4. RESULTS AND DISCUSSION**

**4.1. Homomorphic encryption algorithms in secure cloud-based mental health EHRs promote confidentiality and collaboration**

In mental health care, seamless technological integration has revolutionised EHRs with cloud-based solutions. Homomorphic encryption algorithms (HEAs) may change secure cloud-based mental health EHRs by ensuring confidentiality and fostering cooperation. This study illuminates how HEAs might protect patient privacy by diving into their complexities. Advanced encryption and cloud technologies secure mental health records and enable healthcare providers to collaborate. This paradigm change provides unprecedented opportunity to improve patient care, research, and mental health support, advancing a more secure and linked healthcare environment. Figure 5 shows age, blood pressure (BP), glucose, and heart rate for five individuals. The data is essential for homomorphic encryption of EHRs. To protect privacy and comply with healthcare standards, cloud-based systems must securely store and handle patient data. Computations on encrypted data provide safe cloud-based analytics without exposing patient data using homomorphic encryption. Table 2

shows how a homomorphic encryption framework for secure cloud-based mental health EHRs handles computational efficiency and complicated system integration issues. This approach protects mental health practitioners' collaborative data analysis. Encrypted data calculations protect privacy, enable safe healthcare professional exchange, and reduce unauthorized access threats. This strong method ensures cloud security and collaboration for sensitive mental health data.

Figure 6 adds cholesterol, body mass index (BMI), smoking status, and medication adherence to patient health indicators. Comprehensive health monitoring and personalized therapy need this expanded dataset. This sensitive data may be safely stored and handled in the cloud using homomorphic encryption. Encrypting the data keeps it private while enabling healthcare practitioners to examine and operate on it. This improves data security and privacy, which is essential for digital health system trust.

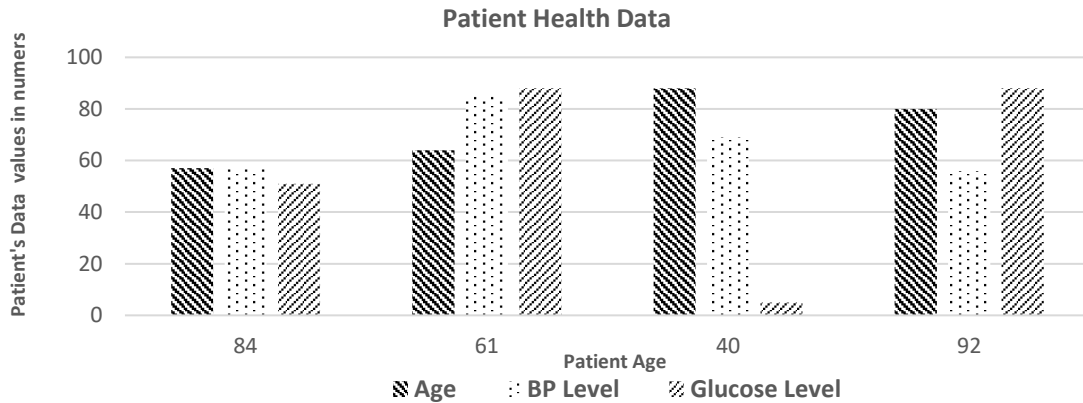


Figure 5. Basic patient health data

Table 2. Homomorphic encryption framework for secure cloud-based EHRs in mental health

Aspect	Challenges	Applications	Advantages
Fully homomorphic encryption	Limited computational efficiency	Secure cloud-based EHRs for mental health	Confidentiality preservation for sensitive mental health data
Partially homomorphic encryption	Complex integration with existing systems	Collaborative data analysis in a secure environment	Privacy-preserving computations on encrypted data
Homomorphic signature schemes	Balancing security and usability	Enabling secure sharing among healthcare professionals	Mitigating risks associated with unauthorized data access

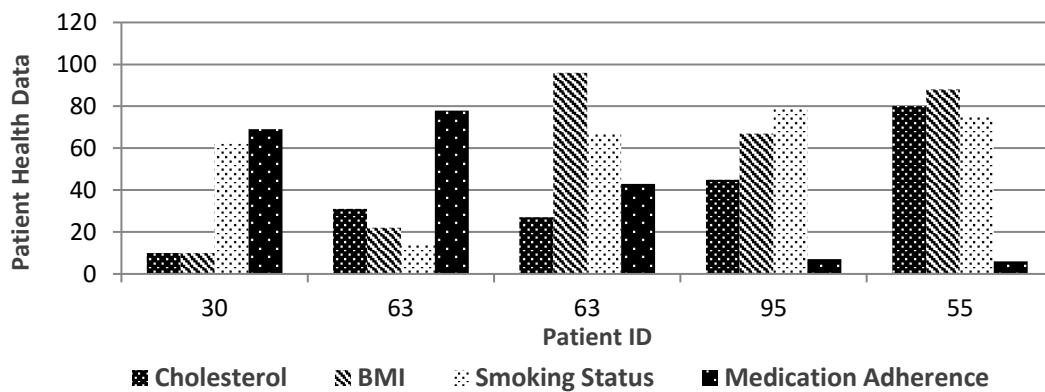


Figure 6. Extended patient health data

**4.2. Secure cloud-based mental health records with homomorphic signature schemes and encryption algorithms**

Advanced cryptography is essential for safe cloud-based mental health EHRs. Homomorphic signature schemes and encryption algorithms have a major influence on healthcare confidentiality and cooperation. Homomorphic signature schemes allow calculations on encrypted data without decrypting

sensitive data, protecting cloud-based EHR privacy. This paradigm is strengthened by homomorphic encryption algorithms, which safeguard mental health data and enable cooperation without sacrificing privacy. This exploration of these cryptographic tools illuminates their potential to transform the security landscape of cloud-based EHRs in mental health, contributing to the ongoing discussion on protecting sensitive healthcare data in a connected digital age. Table 3 shows how homomorphic encryption protects sensitive data like EHRs in cloud settings while meeting tight regulatory requirements. It prevents data breaches and unauthorized access by protecting data during operations. Its implementation is complicated by higher computing complexity, slower processing rates for complex processes, and expensive setup costs. Despite these shortcomings, encryption technologies are improving healthcare IT system scalability, operational efficiency, and flexibility, making homomorphic encryption a potential alternative for protecting patient data in the digital healthcare environment.

Table 3. Homomorphic encryption algorithm

Aspect	Pros	Cons
Security	Protects data confidentiality	Increased computational complexity and resource usage
Privacy	Enables secure data processing	Slower performance compared to plaintext operations
Compliance	Facilitates adherence to regulatory standards	Requires specialized knowledge for implementation
Data integrity	Maintains integrity of encrypted data	Limited support for certain types of computations
Scalability	Supports scalable solutions	Initial setup costs and integration complexities
Flexibility	Allows for flexible data utilization	Potential constraints in handling large datasets
Cost-effectiveness	Reduces risks of data breaches and fines	High computational and operational costs
User accessibility	Enables secure access to sensitive data	Requires robust key management and access controls

#### 4.3. Securing mental health cloud-based EHRs with homomorphic hash functions and encryption algorithms

Advanced cryptography is essential for safe cloud-based mental health EHRs. This article discusses how homomorphic hash functions and encryption techniques help healthcare institutions maintain confidentiality and cooperation. The story explains how these cryptographic approaches protect patient data and facilitate healthcare stakeholder engagement. Beyond traditional encryption, homomorphic techniques that allow computation on encrypted data are highlighted. These advances strengthen EHR security and enable innovative mental health research and treatment collaborations, ensuring that sensitive information remains confidential without slowing collaboration in the ever-changing healthcare informatics landscape. Using homomorphic encryption to secure cloud based EHRs is detailed in the Table 4.

Table 4. Secured and cloud-based electronic health records by homomorphic encryption algorithm

Aspect	Problem statement	Proposed solution	What is new
Data Privacy	Unauthorized access to sensitive patient information in EHRs	Advanced homomorphic encryption techniques to protect data confidentiality	Next-generation homomorphic encryption allowing complex computations on encrypted data without compromising privacy
Data Integrity	Risks of data tampering leading to incorrect diagnoses and treatments	Cryptographic hash functions and digital signatures to ensure data remains unaltered	Enhanced integrity verification mechanisms to detect unauthorized changes in EHRs
Scalability	Handling large volumes of health data without performance degradation	Scalable homomorphic encryption frameworks utilizing parallel processing	Scalable encryption frameworks designed for large-scale health data with optimized cryptographic structures
Computational Overhead	High computational complexity hindering real-time data access	Optimization using hardware accelerators like GPUs and specialized processors	Efficient algorithms and hardware acceleration reducing computational overhead
Regulatory Compliance	Ensuring encryption methods meet legal standards like HIPAA	Built-in compliance tools and regular audits	Integrated compliance features within encryption systems for seamless legal adherence
Interoperability	Difficulty in sharing encrypted data across different EHR systems	Standardized protocols for encrypted data exchange	Establishment of interoperability standards for secure data sharing between various healthcare providers
User Accessibility	Balancing security with ease of access for healthcare providers	Role-based access controls (RBAC) and multi-factor authentication (MFA)	Optimized user access controls balancing security and usability
Disaster Recovery	Secure backup and reliable recovery of encrypted EHRs in case of data loss	Advanced secure backup and disaster recovery solutions	Innovative secure backup solutions ensuring data integrity and reliability
Cost of Implementation	Financial burden of implementing advanced encryption algorithms	Cost-effective cryptographic solutions using open-source libraries and cloud services	Cost-efficient encryption models leveraging open-source and cloud-based services

It highlights data privacy, integrity, scalability, and regulatory compliance issues. Advanced homomorphic encryption, cryptographic hash algorithms, scalable frameworks, and built-in compliance tools are suggested. Next-generation encryption, optimized algorithms for real-time processing, standardized interoperability protocols, and cost-effective cryptographic models are emphasized. Improved user access restrictions, key management, and EHR integration are also stressed. Active maintenance and new latency reduction approaches secure and handle data efficiently. These initiatives attempt to protect, efficiently, and compliantly manage sensitive patient data on the cloud.

## 5. CONCLUSION

The use of homomorphic encryption to secure cloud-based EHRs has pros and cons. Implementing encryption techniques in major healthcare systems is computationally and performance-intensive. Despite these challenges, improved data security and privacy boost patient and provider trust. Scalability and interoperability difficulties highlight the need for healthcare IT technology improvements and standardisation. Future work includes optimising homomorphic encryption algorithms for performance and usability in varied healthcare contexts. Research and development in this area will improve EHR security and ensure regulatory compliance. Successful homomorphic encryption integration will transform EHR administration, creating a more secure and efficient digital healthcare environment. Results from dataset of patient health metrics show in the 1st instance sample data for 5 instances with ages between 57 to 88, BP values from 33 to 85, glucose values from 5 to 99, and heart rate values from 24 to 88. In another study of 5 patients, cholesterol levels ranged from 10 to 80 mg/dL, BMI from 10 to 96 kg/m<sup>2</sup>, smoking status from 14 to 79, and medication adherence from 6 to 78%.

## REFERENCES




- [1] A. Malik, N. Ratha, B. Yalavarthi, T. Sharma, A. Kaushik, and C. Jutla, "Confidential and protected disease classifier using fully homomorphic encryption," in *Proceedings - 2024 IEEE Conference on Artificial Intelligence, CAI 2024*, 2024, pp. 365–370, doi: 10.1109/CAI59869.2024.00074.
- [2] T. Suneetha and D. J. Bhagwan, "A secure framework for enhancing data privacy and access control in healthcare cloud management systems," *Educational Administration Theory and Practices*, vol. 30, no. 5, pp. 13341–13349, 2024, doi: 10.53555/kuey.v30i5.5783.
- [3] K. P. Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, and V. Jha Pillai, "Secure approach to sharing digitized medical data in a cloud environment," *Data Science and Management*, vol. 7, no. 2, pp. 108–118, 2024, doi: 10.1016/j.dsm.2023.12.001.
- [4] K. Rao, "Research on preventing medical information from leaking based on homomorphic encryption," *Frontiers in Computing and Intelligent Systems*, vol. 7, no. 1, pp. 34–38, 2024, doi: 10.54097/wsk1dv30.
- [5] G. R. Ramesh and E. Rajesh, "Secure E-health management automated insights generation for datasets classifications in machine learning on cloud framework," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 10s, pp. 239–252, 2024.
- [6] R. Reddy Palle, R. Palle, and A. Punitha, "Privacy-preserving homomorphic encryption schemes for machine learning in the cloud," *Article in ESP Journal of Engineering & Technology Advancements*, 2021.
- [7] E. Frimpong, K. Nguyen, M. Budzys, T. Khan, and A. Michalas, "GuardML: efficient privacy-preserving machine learning services through hybrid homomorphic encryption," in *Proceedings of the ACM Symposium on Applied Computing*, 2024, pp. 953–962, doi: 10.1145/3605098.3635983.
- [8] S. A. Rieyan *et al.*, "An advanced data fabric architecture leveraging homomorphic encryption and federated learning," *Information Fusion*, vol. 102, 2024, doi: 10.1016/j.inffus.2023.102004.
- [9] H. M. Yousif and S. M. Hameed, "Preserving genotype privacy using AES and partially homomorphic encryption," *Iraqi Journal of Science*, vol. 65, no. 3, pp. 1663–1678, 2024, doi: 10.24996/ijcs.2024.65.3.38.
- [10] K. Yuan *et al.*, "Multiple time servers timed-release encryption based on Shamir secret sharing for EHR cloud system," *Journal of Cloud Computing*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00676-y.
- [11] S. Pothireddy, N. Peddisetty, P. Yellamma, G. Botta, and K. N. Gottipati, "Data security in cloud environment by using hybrid encryption technique: a comprehensive study on enhancing confidentiality and reliability," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 2, pp. 159–170, 2024, doi: 10.22266/ijies2024.0430.14.
- [12] Z. Sultana and D. Kumar, "Medical data privacy representation with improved encryption algorithm," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 8s, pp. 581–591, 2024.
- [13] V. Ananthakrishna and C. S. Yadav, "Innovations in cloud security: enhanced hybrid encryption approach with authprivacychain for enhanced scalability," *Nanotechnology Perceptions*, vol. 20, no. S2, pp. 560–577, 2024, doi: 10.62441/nano-ntp.v20iS2.42.
- [14] Y. Gao, G. Quan, S. Homsy, W. Wen, and L. Wang, "Secure and efficient general matrix multiplication on cloud using homomorphic encryption," *Journal of Supercomputing*, pp. 1–16, 2024, doi: 10.1007/s11227-024-06428-8.
- [15] B. Anantharam, "Privacy-preserving in cloud computing for data storage security framework using regenerating," *International Journal of Computer Engineering and Technology (IJCET)*, vol. 15, no. 1, pp. 90–100, 2024.
- [16] E. Knight, I. Yolou, J. Li, C. Kockan, M. Jensen, and M. Gerstein, "Homomorphic encryption: an application to polygenic risk scores," *bioRxiv*, pp. 1–25, 2024, doi: 10.1101/2024.05.26.595961.
- [17] K. Sravanthi and P. C. Sekhar, "An efficient integrity verification based multi-user cloud access control framework using block chain technology on EHR database," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 9, pp. 536–549, 2024.
- [18] D. J. Dr. Jayarajan, "Efficient privacy preserving medical diagnosis on edge computing platforms," *Journal of Science and Technology*, vol. 9, no. 1, pp. 1–10, 2024, doi: 10.46243/jst.2024.v9.i1.pp1-10.
- [19] C. Gouert and N. G. Tsoutsos, "Data privacy made easy: enhancing applications with homomorphic encryption," *Cryptology ePrint Archive*, pp. 1–37, 2024. Accessed: Mar 16, 2024. [Online], Available: <https://ia.cr/2024/118>






- [20] S. Fugkeaw, L. Hak, and T. Theeramunkong, "Achieving secure, verifiable, and efficient boolean keyword searchable encryption for cloud data warehouse," *IEEE Access*, vol. 12, pp. 49848–49864, 2024, doi: 10.1109/ACCESS.2024.3383320.
- [21] J. Fadhil and S. R. M. Zeebaree, "Blockchain for distributed systems security in cloud computing: a review of applications and challenges," *Indonesian Journal of Computer Science*, vol. 13, no. 2, 2024, doi: 10.33022/ijcs.v13i2.3794.
- [22] N. D. C. Barus and N. F. Barus, "Development of data security algorithms: a literature review on information security in the context of big data," *Journal Islamic Global Network for Information Technology and Entrepreneurship*, vol. 2, no. 1, 2024.
- [23] Oluwabunmi Layode, Henry Nwapali Ndidi Naiho, Gbenga Sheriff Adeleke, Ezekiel Onyekachukwu Udeh, and Talabi Temitope Labake, "Data privacy and security challenges in environmental research: approaches to safeguarding sensitive information," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 6, pp. 1193–1214, 2024, doi: 10.51594/ijarss.v6i6.1210.
- [24] S. Salih and Subhi R. M. Zeebaree, "Unveiling the synergistic relationship between distributed systems and cloud computing: a review of architectural trends," *Indonesian Journal of Computer Science*, vol. 13, no. 2, pp. 2206–2221, 2024, doi: 10.33022/ijcs.v13i2.3801.
- [25] S. Vadim, M. Firdaus, and K.-H. Rhee, "Privacy-preserving decentralized biometric identity verification in car-sharing system," *Journal of Multimedia Information System*, vol. 11, no. 1, pp. 17–34, 2024, doi: 10.33851/jmis.2024.11.1.17.
- [26] S. Selvarasu, K. Bashkaran, K. Radhika, S. Valarmathy, and S. Murugan, "IoT-enabled medication safety: real-time temperature and storage monitoring for enhanced medication quality in hospitals," in *2nd International Conference on Automation, Computing and Renewable Systems*, 2023, pp. 256–261, doi: 10.1109/ICACRS58579.2023.10405212.
- [27] R. Raman, K. Dhivya, P. Sapra, S. Gurpur, S. P. Maniraj, and S. Murugan, "IoT-driven smart packaging for pharmaceuticals: ensuring product integrity and patient safety," 2023, doi: 10.1109/ICAIIH157871.2023.10489420.
- [28] A. Deepa, R. Latha, T. S. Kumar, N. K. Manikandan, J. Preetha, and S. Murugan, "IoT-based wearable devices for personal safety and accident prevention systems," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, 2023, pp. 1510–1514, doi: 10.1109/SmartTechCon57526.2023.10391691.
- [29] K. Padmanaban, A. M. Senthil Kumar, H. Azath, A. K. Velmurugan, and M. Subbiah, "Hybrid data mining technique based breast cancer prediction," 2023, doi: 10.1063/5.0110216.
- [30] M. Senthil Kumar, H. Azath, A. K. Velmurugan, K. Padmanaban, and M. Subbiah, "Prediction of alzheimer's disease using hybrid machine learning technique," in *AIP Conference Proceedings*, 2023, vol. 2523, doi: 10.1063/5.0110283.
- [31] B. J. Ganesh, P. Vijayan, V. Vaidehi, S. Murugan, R. Meenakshi, and M. Rajmohan, "SVM-based predictive modeling of drowsiness in hospital staff for occupational safety solution via IoT infrastructure," 2024, doi: 10.1109/IC457434.2024.10486429.

## BIOGRAPHIES OF AUTHORS






**Bala Annapurna**    is an associate professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh. She is a dedicated educator and a passionate researcher in the field of computer science and engineering. She has been actively engaged in academic and research endeavors for more than twenty years, making substantial contributions to the scholarly community during this time. Her research interests encompass a wide range of topics in computer science and engineering, with a specific focus on data mining. She is deeply engaged in research areas such as clustering and regression analysis and has a strong commitment to pushing the boundaries of knowledge in these fields. She has authored and co-authored numerous research papers in renowned computer science and engineering journals and conferences. She actively engages with the industry and the academic community through collaborative research projects and consulting work. This practical experience allows her to bridge the gap between theoretical knowledge and real-world applications in the field of computer science engineering. She can be contacted at email [annapurnagandrey@gmail.com](mailto:annapurnagandrey@gmail.com).






**Gaddam Geetha**    received B.Tech. degree in 2010 in computer science and engineering from Institute of Aeronautical Engineering and Technology. M.Tech. degree in 2013 in computer science and engineering from Institute of Aeronautical Engineering and Technology and pursuing Ph.D. in Computer Science and Engineering from SRM University. She is in teaching profession for past 10 years. She published 10 papers in international journals and conferences. She can be contacted at email: [geethareddy0412@gmail.com](mailto:geethareddy0412@gmail.com).






**Priyanka Madhiraju**    is an assistant professor at Matrusri Engineering College since 2015. She has 11 years of teaching experience. She completed her M.Tech. from Jagruthi Institute of Engineering and Technology (2011-2013), undergraduate from Sindhura College of Engineering and Technology (2003-2007). Her research interests are cloud computing and blockchain technology. She has attended 20+ faculty development programs, international conferences and workshops. She has published 10 research papers in various national and international reputed journals. She can be contacted at: [priyankaraomadhiraju@gmail.com](mailto:priyankaraomadhiraju@gmail.com).






**Subbarayan Kalaiselvi**    received the Master of Computer Applications in the year 1998, M.Phil. degree in the year 2004 from Bharathiar University. Completed Master of Engineering in computer science in the year 2006 and Ph.D. in the year 2021 in Anna University, Chennai. Presented more than 20 papers in national, international conferences and published 15 papers in international journals. Completed DST sponsored research project and organized seminars and career oriented programme sponsored by UGC, AICTE, and DBT. Currently working as an associate professor and head in the department of computer technology at Kongu Engineering College, Erode. Research interest includes computer networks and cloud computing. She can be contacted at email: kalai.ctug@kongu.edu.






**Mishmala Sushith**    has completed her Ph.D. in information and communication engineering in the area of image processing from Anna University, Chennai. She completed her M.E. in computer science and engineering from SNS College of Engineering and Technology and B.E. in computer science and engineering from Mepco Schlenk Engineering College, Sivakasi. She has 20 years of teaching experience in Engineering college and 7 years of industrial experience. She is currently working as a professor and head in the Department of Information Technology in Adithya Institute of Technology. Her research interests include internet of things, networking, cyber security and data analytics. She has published more than 50 papers in refereed international journal and conferences. She is a MCSE 2003 professional. She has published one patent and is an editor in IRO journals. She can be contacted at email: mishmala@gmail.com.



**Rathinasabapathy Ramadevi**    completed her Ph.D. specialization on condition monitoring using computational intelligence. Her research interests include instrumentation, condition monitoring, signal/image processing and analysis, applications of artificial neural network, fuzzy logic and wavelet transform. She has more than 25 years of teaching and research experience and authored nearly 50 research articles/books in reputed journals/conferences in these fields. She is serving as an editorial member and reviewer of several national/international reputed journals. Dr. R. Ramadevi is the member of many international affiliations. She can be contact at email: ramadevir.sse@saveetha.com.



**Pramod Pandey**    was born in India in 1975. He received his M.Tech. and Ph.D. degree from Indian Institute of Technology Kanpur India in 2004 and 2012 respectively. He has worked as scientist at Korea Atomic Energy Research Institute Daejeon South Korea, Marie Curies Post-Doctoral fellow at DCU Dublin Ireland, Research Establishment Officer at IIT Kanpur, and has R&D industrial experience in design and development of ophthalmic instruments. Presently he is working as assistant professor at Symbiosis Institute of Technology Nagpur. Apart from this Dr. Pandey has worked in several other projects funded from Science Foundation Ireland and European Union Commission. Dr. Pandey is trained laser safety officer, from Pro-Lite Technology Ltd, Innovation Centre, Cranfield University United Kingdom. He is a member of IEEE and has about 13 international journal publications in reputed journals and attended about 25 international and national conferences. His research interest includes laser plasma applications in industries and medical fields and many more related fields. He can be contact at email: pramod.pandey@sitnagpur.siu.edu.in.