A Review of Homomorphic Encryption and its Contribution to the Sector of Health Services

Fotios Roumpies*
Dpt. of Computer Science and Biomedical Informatics,
University of Thessaly
Lamia, Greece
froumpies@uth.gr

Athanasios Kakarountas*
Dpt. of Computer Science and Biomedical Informatics,
University of Thessaly
Lamia, Greece
kakarountas@uth.gr

ABSTRACT

Homomorphic encryption is a groundbreaking cryptographic method that has made giant contributions to healthcare by addressing the urgent need for steady and privacy-keeping information analysis and sharing. This encryption approach permits information to be processed while nonetheless in its encrypted form, permitting healthcare businesses to perform complex computations on confidential patient information without compromising character privacy or data protection. It paved the way for secure cloud-based facts storage, sharing, and collaborative healthcare research, facilitating advancements in fact-driven selection-making, customized medicinal drugs, and remote affected person tracking. Homomorphic encryption has emerged as a vital enabler of innovation by maintaining the confidentiality of affected personal information while enabling meaningful analysis.

CCS CONCEPTS

• **Security and privacy** → **Cryptography**; *Social aspects of security and privacy*; • **Applied computing** → *Health care information systems.*

KEYWORDS

Homomorphic Encryption, Healthcare, secure data sharing, digital libraries, data security

ACM Reference Format:
Fotios Roumpies and Athanasios Kakarountas. 2023. A Review of Homomorphic Encryption and its Contribution to the Sector of Health Services. In *27th Pan-Hellenic Conference on Progress in Computing and Informatics (PCI 2023), November 24–26, 2023, Lamia, Greece.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3635059.3635096

1 INTRODUCTION

In an age wherein statistics fuel innovation and power essential choice-making tactics throughout various sectors, ensuring the privacy and security of sensitive statistics has become paramount. Homomorphic encryption, a leap-forward concept, conceived in 1978, remained theoretical for many years, through the boundaries of what seemed attainable in secure data processing. This literature review depicts a degree of the comprehensive journey into the sector of homomorphic encryption, its applications, demanding situations, and the future it shapes in the area of secure records, intending at the same time to offer insights into its contribution to the healthcare sector. In the first part of this paper, an introduction to the modern-day cryptographic approach is made, which is a sentinel at the intersection of record safety, computational performance, and its profound effect on our potential to carry out secure record processing while retaining data confidentiality. In the second part (STATE OF THE ART) we describe the current knowledge about the studied matter through the analysis of similar or related published work [2]. It is also emphasized that it has unexpectedly advanced from a theoretical curiosity into a sensible answer with profound implications for numerous domains, representing a revolutionary paradigm shift within the area of cryptography. The third part refers to the most important tools of homomorphic encryption in the healthcare sector and its implementation in data security. Moving forward to the fourth part, we discuss health data security as well as regulatory and legal considerations. Finally, in the fifth part, conclusions are presented, and future direction and scope are mentioned. On an overall basis, this literature review depicts a degree of the comprehensive journey into the sector of homomorphic encryption, its applications, demanding situations, and the future it shapes in the area of secure records, intending at the same time to offer insights into its contribution to the healthcare sector.

This work is licensed under a Creative Commons Attribution International 4.0 License.

PCI 2023, November 24–26, 2023, Lamia, Greece
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1626-3/23/11.
https://doi.org/10.1145/3635059.3635096

2 STATE OF THE ART

The possibility of homomorphic encryption was proposed by Rivest, Adleman and Dertouzos (1978) while it was discovered that many schemes supported either multiplication or addition, including RSA (Rivest, Shamir, and Adleman, 1978), ElGamal (ElGamal, 1985), and Goldwasser-Micali (Goldwasser and Micali, 1982), Paillier (Paillier, 1999), among others. However, many of them had restrictions on finding a feasible system. The three-decade-old issue wasn't resolved until Gentry's landmark 2009 study, in which he demonstrated a feasible system meeting all the requirements [1].

Partial homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), and Fully homomorphic encryption (FHE) are the three kinds of homomorphic encryption. On the basis of encryption, decryption, difficulty, and homomorphic quality, several partial homomorphic encryption techniques are contrasted. Somewhat homomorphic encryption (SWHE) examines the circuit up to a certain depth or limit and supports a certain number of operations. Over encrypted data, FHE allows actions to be held

an unlimited number of times. Whereas Fully Homomorphic Encryption (FHE), permits an infinite number of arbitrary operations over ciphertext, SWHE is a more limited solution. SWHE is able to manage a certain amount of processes across the ciphertext, or it can deal with multiplication and addition processes separately but not simultaneously. [19]. In Figure 3 there is a historical retrospect of the above-mentioned encryptions, and table 1 presents a timeline of milestones in homomorphic encryption schemes.

The core precept of homomorphic encryption lies in its potential to carry out operations on ciphertexts so that the decrypted results are consistent with the operations carried out on the plaintext information. In other words, it is possible to upload, multiply, or perform other mathematical operations on encrypted data, and the final results stay confidential. These belongings unlock many opportunities in an era when data privacy is paramount, and information sharing for collaborative studies, cloud computing, and steady healthcare programs is imperative [9]. In steady facts outsourcing, this novelty gave the chance to corporations to offload records to outside companies for processing without revealing their contents. This is a game-changer for agencies that seek to leverage the computational electricity of the cloud while keeping strict manipulation of oversensitive facts. Meanwhile, the healthcare zone has embraced homomorphic encryption as an essential device for allowing stable and privacy-preserving data analysis [3].

Researchers and healthcare companies carry out complicated analytics on affected personal data without exposing personal clinical records, paving the way for personalized medicine and collaborative studies initiatives. This no longer only hurries up clinical breakthroughs but also safeguards affected person privacy in an era when statistics breaches are a consistent threat. In the financial sector, homomorphic encryption is being hired to guard sensitive economic transactions and consumer statistics, even while still taking into consideration efficient facts evaluation and fraud detection. Similarly, governments and intelligence organizations are exploring its application in securing confidential records [8].

This groundbreaking cryptographic technique has garnered great interest in the healthcare industry due to its potential to deal with privacy and protection concerns while facilitating statistics-pushed choice-making and collaborative studies. Numerous previous studies, through their findings, have highlighted the critical function of homomorphic encryption in safeguarding sensitive affected personal records in various public and private sectors [11].

As healthcare organizations increasingly adopt digital fitness statistics and share statistics for studies and scientific purposes, worries concerning statistics privacy have grown. Homomorphic encryption allows for stable facts sharing and analysis without the need to decrypt sensitive patient data, thereby lowering the threat of breaches and unauthorized access *(e.g. cybersecurity attacks)*. The homomorphic encryption tool used in stable data analytics is a crucial area of focus in the literature. Researchers have confirmed how homomorphically encrypted data can be used for diverse healthcare analytics duties, including predictive modeling, sickness surveillance, and affected person final results evaluation [13].

Additionally, it is emphasised the ability to derive precious insights from encrypted facts while preserving patient confidentiality. Furthermore, the integration of homomorphic encryption with machine-studying algorithms has won interest as it permits the development of privacy-retaining AI fashions for the healthcare sector. This method allows healthcare establishments to collaborate on constructing predictive models or sharing patient statistics with AI-driven packages, in a secure environment. Researchers have explored how this mixture can enhance diagnostic accuracy, remedy suggestions, and patient care. In healthcare statistics sharing, homomorphic encryption has been examined to permit steady move-institutional collaborations and federated knowledge. As shown in Figure 1, the literature describes how healthcare providers, pharmaceutical firms, and academic institutions have used homomorphic encryption to aggregate their data assets for extensive research while upholding stringent confidentiality requirements [15].

As we delve deeper into this homomorphic encryption exploration, it becomes glaring that this cryptographic surprise goes beyond technological innovation; it redefines the limits of what is viable within data privacy and protection. While the advantages of homomorphic encryption in healthcare are prominent, challenges are also discussed, like computational overhead. Researchers have explored strategies to mitigate this problem, including optimizing algorithms and leveraging hardware acceleration. The literature on homomorphic encryption's contribution to the healthcare sector underscores its potential to revolutionize statistics, privacy, and safety within the healthcare industry [16].

By permitting secure statistics sharing, evaluation, and collaborative research, homomorphic encryption paves the manner for advancements in personalized medicine, disorder prevention, and healthcare innovation. However, addressing computational demanding situations and standardization problems remains a priority for destiny studies and realistic implementation in healthcare settings.

3 IMPLEMENTATIONS AND TOOLS OF HOMOMORPHIC ENCRYPTION IN HEALTHCARE SECTOR

A number of essential additives are included in a practical homomorphic encryption implementation. First and foremost, the integration of homomorphic encryption into packages is made simpler by specific libraries and toolkits. These libraries, including the Simple Encrypted Arithmetic Library (SEAL) from Microsoft and the Homomorphic Encryption Toolkit (HELib) from IBM, offer prebuilt functionalities and APIs for interacting with encrypted data. These assets often guide various encryption schemes and provide optimizations to enhance overall performance, making it viable for developers to include homomorphic encryption seamlessly. Secondly, international programs in sectors like healthcare, finance, and secure information sharing are instrumental in showcasing the electricity of homomorphic encryption [23]

Healthcare programs rent this cryptographic approach to evaluate secure clinical information while retaining patient privacy. These packages regularly rely upon homomorphic encryption libraries to force the desired cryptographic operations, ensuring sensitive medical facts remain personal. Moreover, databases have evolved to deal with homomorphic encryption, allowing organizations to keep secure and question encrypted records. Systems like CryptDB (a system that provides practical and provable confidentiality to face attacks for applications backed by SQL databases), and Mylar (a research platform for building web applications with

Table 1: TIMELINE OF MILESTONES IN HOMOMORPHIC ENCRYPTION SCHEMES

Year and Scheme	Homomorphic Encryption applications
RSA, 1978	Banking and credit card transaction [20]
ElGamal, 1985	In Hybrid Systems [20]
Paillier, 1999	E-Voting [20]
WSNs, 2007	Computing Aggregation Function Minimum/Maximum using HE Schemes in W.S.Ns Cryptosystem [25]
BGV, 2011	For the security of integer polynomials [20]
FHEW, 2014	TFHE: Fast Fully Homomorphic Encryption over the Torus [5]
CKKS, 2016	Homomorphic Machine Learning Big Data Pipeline for the Financial Services Sector [17]
TFHE, 2020	An homomorphic LWE based E-voting Scheme [5]

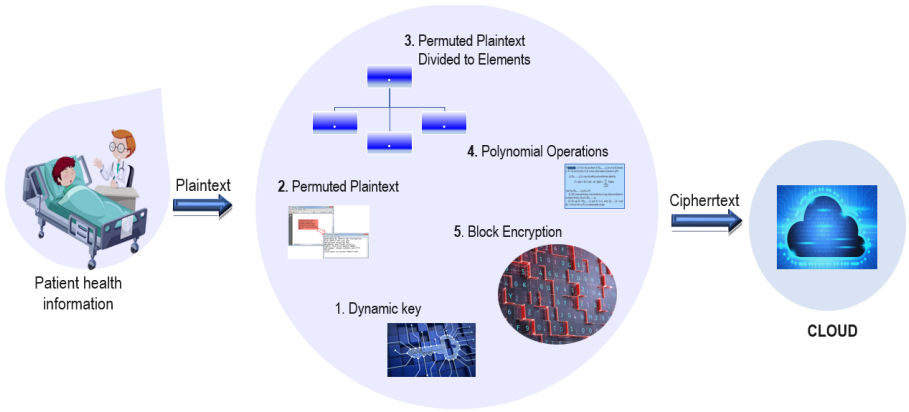

Figure 1: Homomorphic Encryption in the healthcare system

end-to-end encryption) have emerged as exemplars in this space. They leverage homomorphic encryption techniques to protect data at rest while enabling efficient and steady record retrieval and querying. These databases provide the crucial infrastructure for groups looking to shield sensitive records. Many tutorial sources are available online to facilitate the adoption and expertise of homomorphic encryption. These materials (depicted as an example in Figure 2), offer complete insights into homomorphic encryption concepts and realistic elements, often observed with code examples and high-quality practices tailored to numerous scenarios [14].

Homomorphic encryption, a modern-day cryptographic method, has emerged as a sport-changing solution in the healthcare industry by way of addressing the vital mission of balancing statistics' privateness and accessibility. In healthcare, in which sensitive patient statistics are ubiquitous and essential for scientific studies and treatment, homomorphic encryption enables steady computations on encrypted facts without requiring decryption, thereby keeping the privacy of affected personal data. This innovation has sizable implications for healthcare companies, facilitating stable statistics sharing and collaboration amongst healthcare providers, researchers, and establishments while ensuring compliance with stringent statistics safety guidelines like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the EU general data protection regulation (GDPR) [21].

Moreover, homomorphic encryption empowers advanced analytics, including systems gaining knowledge of encrypted healthcare data, imparting a unique opportunity for medical breakthroughs without compromising privacy. As telemedicine and remote-affected person monitoring keep expanding, this technology ensures the confidentiality and integrity of patient data throughout far-off consultations. Homomorphic encryption speeds up medical research and ultimately helps the transformation of the healthcare enterprise environment by reducing the dangers associated with data breaches and illegal admittance. [4].

4 HEALTHCARE DATA SECURITY

Healthcare statistics protection is a paramount problem in the current healthcare panorama, where touchy affected person information is digitized, saved, and transmitted across a complicated atmosphere of healthcare vendors, insurance groups, researchers, and administrators. The significance of strong information security cannot be overstated, as healthcare data is a high goal for cybercriminals because of its gigantic value in the black marketplace and the capacity for identity theft, fraud, or even damage to patients. One of the foundational factors of healthcare records protection is encryption [22].

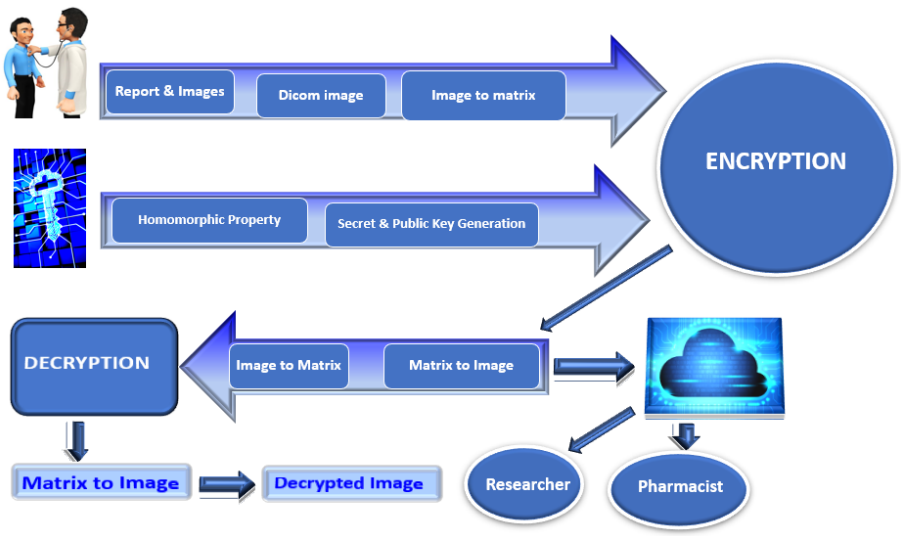

Figure 2: Framework of homomorphic cryptography in the Sector of Health Services *(based on [26])*

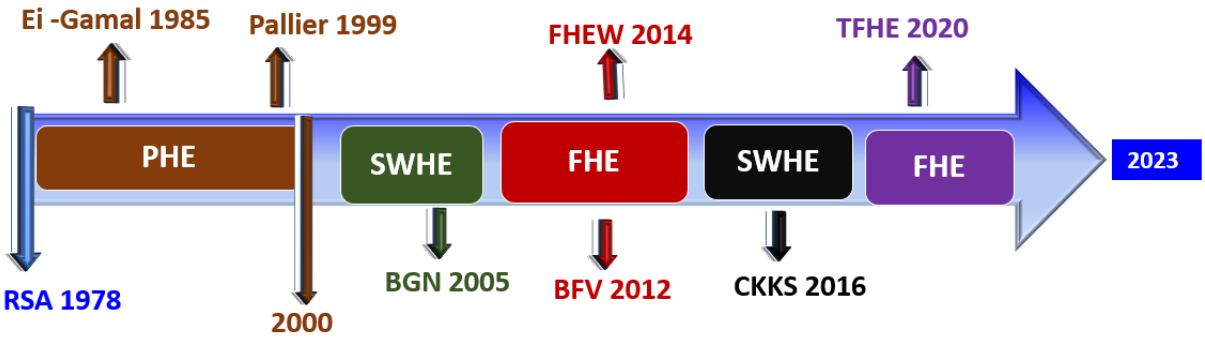

Figure 3: Timeline of several important HE schemes*(based on [6])*

Data encryption ensures that affected-person records, diagnostic results, and other medical information remain private and unintelligible to unauthorized users. In this context, homomorphic encryption has gained prominence for its capability to enable secure computations on encrypted data, permitting healthcare professionals and researchers to analyze confidential data without compromising affected personal privacy. Beyond encryption, healthcare records protection contains a multi-faceted method that consists of getting the right of entry to controls, authentication mechanisms, and normal security audits [18].

Access controls make certain that the handiest authorized personnel can get the right of entry to affected person facts, even robust authentication mechanisms like biometrics or multi-factor authentication (MFA) upload an extra layer of safety. Regular protection audits and vulnerability tests are vital to discover and mitigate capacity weaknesses inside the safety infrastructure. Additionally, the healthcare industry must live vigilant against evolving cybersecurity threats which include ransomware assaults, phishing attempts, and insider threats. Developing a secure digital perimeter in every sensitive facility and updating robust incident response plans is critical to increasing deterrence, minimizing the impact of a safety breach, and making sure of quick healing [27].

These guidelines outline strict suggestions for protecting the affected person's facts, implementing criminal responsibilities, and severe consequences for non-compliance. Healthcare information safety is a multifaceted task that necessitates a mixture of encryption, right of entry to controls, authentication, regular audits, and compliance with stringent guidelines. The adoption of progressive encryption techniques like homomorphic encryption is indicative of the healthcare sector's commitment to advancing data protection at the same time as preserving the confidentiality and integrity of patient facts in a more and more virtual and interconnected healthcare atmosphere. Failure to deal with those safety concerns exposes healthcare companies to significant felony, monetary, and reputational risks [28] [7] [24] [26].

4.1 Regulatory Compliance and Legal Considerations

Ensuring regulatory compliance and addressing legal issues is paramount whilst enforcing homomorphic encryption in healthcare. One of the maximum sizeable regulatory frameworks in the United States is HIPAA, which mandates strict requirements for the safety of patient facts and imposes sizable penalties for non-compliance. Homomorphic encryption aligns nicely with HIPAA's necessities, as it permits healthcare agencies to perform important statistics operations while preserving sensitive affected person records exclusively. However, healthcare agencies ought to meticulously plan their implementation approach, ensuring that the encryption scheme selected aligns with HIPAA standards and hints [24]. Additionally, they need to build up reliable access controls and audit trails to monitor data usage and demonstrate compliance.

In our neighborhood, the European Union, the General Data Protection Regulation (GDPR) poses extra challenges and possibilities for healthcare agencies. GDPR enforces stringent facts safety rules, necessitating explicit consent for data processing and stringent rights for facts subjects. Homomorphic encryption can help healthcare organizations comply with GDPR requirements by enabling data analytics without disclosing raw patient data, thereby minimizing the risks associated with records breaches and unauthorized admission [26].

However, as GDPR requirements are tricky and evolving, healthcare corporations need to interact with criminal specialists to ensure full compliance. Moreover, beyond unique rules, healthcare vendors and companies need to recollect broader felony and moral implications related to homomorphic encryption. These considerations embody troubles consisting of liability in the event of a security breach, knowledgeable consent for facts processing, and transparency in statistics usage. Developing clear rules, approaches, and informed consent mechanisms is essential to navigating these legal and ethical complexities effectively [10].

In précis, regulatory compliance and prison concerns are pivotal when adopting homomorphic encryption in healthcare. Compliance with policies like HIPAA and GDPR, coupled with radical know-how of criminal and ethical nuances, not only safeguards patient facts but also fosters belief among sufferers and stakeholders. Healthcare groups must prioritize these factors to harness the total capacity of homomorphic encryption, even as adhering to the evolving criminal panorama governing healthcare information protection [12].

5 CONCLUSIONS

In conclusion, the combination of homomorphic encryption in the healthcare enterprise represents a pivotal step towards achieving the delicate balance between statistics privacy and accessibility in a virtual age.

This cryptographic innovation offers a transformative approach to safeguarding sensitive patient facts even empowering healthcare companies with stable statistics sharing, privateness-keeping analytics, and seamless telemedicine. Its capacity contributions to healthcare are significant, promising advanced affected person care, revolutionary scientific research, and enhanced statistics security.

However, a hit implementation hinges on meticulous interest in regulatory compliance, legal concerns, and the careful navigation of ethical worries. As the healthcare panorama continues to conform, homomorphic encryption stands as a beacon of desire, fostering affected person consideration, accelerating clinical improvements, and riding the healthcare enterprise towards a future where privacy and development coexist harmoniously.

5.1 Future Direction and Scope

The future direction and scope of homomorphic encryption in healthcare are poised for giant expansion and innovation. By permitting secure statistics sharing, evaluation, and collaborative research, homomorphic encryption paves the manner for advancements in personalized medicine, disorder prevention, and healthcare innovation.

Looking in advance, researchers and healthcare agencies are predicted to focus on refining homomorphic encryption algorithms to reduce computational overhead, solve standardization problems, and enhance efficiency, making it extra on hand for real-time clinical applications.

This technology will probably discover broader integration into healthcare structures, inclusive of digital health records, wearable devices, and medical IoT, allowing steady statistics sharing, complete analytics, and remote affected person tracking on an unheard-of scale.

Advances in federated learning (FL) and multi-party computation (MPC), along with homomorphic encryption, could encourage collaborative research endeavors while protecting the confidentiality of information. As regulatory frameworks continue to adapt, compliance strategies for worldwide data safety regulations will remain a focal point. Ethical considerations surrounding patient consent and statistics possession may even drive discussions.

Overall, the destiny of homomorphic encryption in healthcare guarantees a transformative impact, ushering in an era of more suitable affected person care, groundbreaking studies, and fortified statistics safety.

ACKNOWLEDGMENTS

We acknowledge support of this work by the project "ParICT_CENG: Enhancing ICT research infrastructure in Central Greece to enable processing of Big data from sensor stream, multimedia content, and complex mathematical modeling and simulations" (MIS 5047244) which is implemented under the Action "Reinforcement of the Research and Innovation Infrastructure", funded by the Operational Programme "Competitiveness, Entrepreneurship and Innovation" (NSRF 2014-2020) and co-financed by Greece and the European Union (European Regional Development Fund).

REFERENCES

[1] Louis JM Aslett, Pedro M Esperança, and Chris C Holmes. 2015. A review of homomorphic encryption and software tools for encrypted statistical machine learning. *arXiv preprint arXiv:1508.06574* (2015).

[2] Razvan Bocu and Cosmin Costache. 2018. A homomorphic encryption-based system for securely managing personal health metrics data. *IBM Journal of Research and Development* 62, 1 (2018), 1–1.

[3] Rickard Brännvall, Henrik Forsgren, Helena Linge, Marina Santini, Alireza Salehi, and Fatemeh Rahimian. 2022. Homomorphic encryption enables private data sharing for digital health: winning entry to the Vinnova innovation competition Vinter 2021–22. In *2022 Swedish Artificial Intelligence Society Workshop (SAIS)*. IEEE, 1–10.

[4] Sergiu Carpov, Thanh Hai Nguyen, Renaud Sirdey, Gianpiero Constantino, and Fabio Martinelli. 2016. Practical privacy-preserving medical diagnosis using

homomorphic encryption. In *2016 ieee 9th international conference on cloud computing (cloud)*. IEEE, 593–599.

[5] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. 2020. TFHE: fast fully homomorphic encryption over the torus. *Journal of Cryptology* 33, 1 (2020), 34–91.

[6] Thi Van Thao Doan, Mohamed-Lamine Messai, Gérald Gavin, and Jérôme Darmont. 2023. A survey on implementations of homomorphic encryption schemes. *The Journal of Supercomputing* (2023), 1–42.

[7] Nikunj Domadiya and Udai Pratap Rao. 2022. ElGamal Homomorphic Encryption-Based Privacy Preserving Association Rule Mining on Horizontally Partitioned Healthcare Data. *Journal of The Institution of Engineers (India): Series B* 103, 3 (2022), 817–830.

[8] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. 2017. Manual for using homomorphic encryption for bioinformatics. *Proc. IEEE* 105, 3 (2017), 552–567.

[9] Abdelali El Bouchti, Samir Bahsani, and Tarik Nahhal. 2016. Encryption as a service for data healthcare cloud security. In *2016 fifth international conference on future generation communication technologies (FGCT)*. IEEE, 48–54.

[10] Antonio Guimaraes, Leonardo Neumann, Fernanda A Andaló, Diego F Aranha, and Edson Borin. 2022. Homomorphic evaluation of large look-up tables for inference on human genome data in the cloud. In *2022 International Symposium on Computer Architecture and High Performance Computing Workshops (SBAC-PADW)*. IEEE, 33–38.

[11] Bin Jia, Xiaosong Zhang, Jiewen Liu, Yang Zhang, Ke Huang, and Yongquan Liang. 2021. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Transactions on Industrial Informatics* 18, 6 (2021), 4049–4058.

[12] Arun Kumar Jindal, Imtiyazuddin Shaik, Vasudha Vasudha, Srinivasa Rao Chalamala, Rajan Ma, and Sachin Lodha. 2020. Secure and privacy preserving method for biometric template protection using fully homomorphic encryption. In *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*. IEEE, 1127–1134.

[13] Mohd Atif Kaleem, Parvez Mahmood Khan, and Usman Ali Khan. 2021. Strengthening of homomorphic encryption scheme for cloud environment using particle optimization algorithm. In *2021 Fourth international conference on computational intelligence and communication technologies (CCICT)*. IEEE, 397–405.

[14] Ovunc Kocabas and Tolga Soyata. 2015. Utilizing homomorphic encryption to implement secure and private medical cloud computing. In *2015 IEEE 8th International Conference on Cloud Computing*. IEEE, 540–547.

[15] Shancang Li, Shanshan Zhao, Geyong Min, Lianyong Qi, and Gang Liu. 2021. Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things. *IEEE Internet of Things Journal* 9, 16 (2021), 14542–14550.

[16] Mbarek Marwan, Ali Kartit, and Hassan Ouahmane. 2016. Applying homomorphic encryption for securing cloud database. In *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*. IEEE, 658–664.

[17] Oliver Masters, Hamish Hunt, Enrico Steffinlongo, Jack Crawford, Flavio Bergamaschi, Maria E Dela Rosa, Caio C Quini, Camila T Alves, Feranda de Souza, and Deise G Ferreira. 2019. Towards a homomorphic machine learning big data pipeline for the financial services sector. *Cryptology ePrint Archive* (2019).

[18] Souhail Meftah, Benjamin Hong Meng Tan, Chan Fook Mun, Khin Mi Mi Aung, Bharadwaj Veeravalli, and Vijay Chandrasekhar. 2021. Doren: toward efficient deep convolutional neural networks with fully homomorphic encryption. *IEEE Transactions on Information Forensics and Security* 16 (2021), 3740–3752.

[19] Kundan Munjal and Rekha Bhatia. 2023. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems* 9, 4 (2023), 3759–3786.

[20] Payal V Parmar, Shraddha B Padhar, Shafika N Patel, Niyatee I Bhatt, and Rutvij H Jhaveri. 2014. Survey of various homomorphic encryption algorithms and schemes. *International Journal of Computer Applications* 91, 8 (2014).

[21] Jean Louis Raisaro, Gwangbae Choi, Sylvain Pradervand, Raphael Colsenet, Nathalie Jacquemont, Nicolas Rosat, Vincent Mooser, and Jean-Pierre Hubaux. 2018. Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy. *IEEE/ACM transactions on computational biology and bioinformatics* 15, 5 (2018), 1413–1426.

[22] Sogo Pierre Sanon, Rekha Reddy, Christoph Lipps, and Hans Dieter Schotten. 2023. Secure Federated Learning: An Evaluation of Homomorphic Encrypted Network Traffic Prediction. In *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, 1–6.

[23] Muhammad Umair Shaikh, Wan Azizun Wan Adnan, and Siti Anom Ahmad. 2021. Sensitivity and Positive Prediction of Secured Electrocardiograph (ECG) Transmission using Fully Homomorphic Encryption Technique (FHE). In *2020 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES)*. IEEE, 292–297.

[24] V Subramaniyaswamy, V Jagadeeswari, V Indragandhi, Rutvij H Jhaveri, V Vijayakumar, Ketan Kotecha, Logesh Ravi, et al. 2022. Somewhat homomorphic encryption: Ring learning with error algorithm for faster encryption of iot sensor signal-based edge devices. *Security and Communication Networks* 2022 (2022).

[25] E Vaidehi. 2007. Computing aggregation function minimum/maximum using homomorphic encryption schemes in wireless sensor networks (wsns). *California State University, East Bay Hayward, CA, USA* 14 (2007).

[26] AM Vengadapurvaja, G Nisha, R Aarthy, and N Sasikaladevi. 2017. An efficient homomorphic medical image encryption algorithm for cloud storage security. *Procedia computer science* 115 (2017), 643–650.

[27] Sharath Yaji, Kajal Bangera, and B Neelima. 2018. Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications. In *2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*. IEEE, 81–85.

[28] Li Zhang, Jianbo Xu, Pandi Vijayakumar, Pradip Kumar Sharma, and Uttam Ghosh. 2022. Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system. *IEEE Transactions on Network Science and Engineering* (2022).