process that progresses without external help. Modulus switching is another prominent strategy for achieving better asymptotic performance than bootstrapping.

- Step 4: Encrypted results are provided to client.
- Step 5: Client at its end computes decryption using decryption function and recovers f(message).

$$Dec(Enc(f(message))) = f(message)$$

As a result no information is lost by getting encrypted results and decryption at its own end.

Motivation

Security is the key concern in cloud computing. Data provided to third-party service providers for processing and automation are a big issue. Every single business or organization wishes for the personal and sensitive data of the user. Every organization whether government, private, healthcare, academia requires data for policy formation, research purposes, planning new marketing strategies, or launching innovative products. Our main concern is with healthcare privacy as according to a survey by acumen research and consulting [1] healthcare cloud computing market will pass US$ 40 billion by the year 2026. Cloud computing in health care not only increases efficiency but also reduces cost. It is fast but protection of patient-sensitive data is the prime concern as it will not only promote patient confidence but also help in economic development. The digitization of a patient's medical records is supposed to improve care quality and efficiency while reducing costs. On the other hand, patient records include a considerable quantity of sensitive information. As a result, patients must be able to swiftly allow a range of medical affiliates to access their sensitive information using a simple, trustworthy, efficient, and secure approach. Therefore, it is vital to look at the usage of homomorphic encryption in healthcare and compare various homomorphic algorithms for illness prediction as well as data querying while protecting the privacy of patient information.

The rest of this article is organized as follows: the next section contains review methods, planning, inclusion and exclusion criterion, research questions with motivation. The subsequent section compares and analyzes homomorphic encryption starting with partial and somewhat homomorphic encryption approaches followed by fully homomorphic encryption approaches. Techniques to fully homomorphic encryption were classified into four categories, with significant approaches in each category were compared. The next section focuses on homomorphic encryption in the healthcare sector. Homomorphic encryption techniques were compared on the basis of communication and computation overhead for securely identifying LQTC, cancer, average heart rate, cardiovascular problems, and a secure query generating system in healthcare. Finally, conclusion is presented.

Review method

The systematic review process may be considered as a means of solving a specific research problem. Presently no systematic reviews are focusing on homomorphic cryptosystems in healthcare and bioinformatics, therefore a systematic review research methodology was chosen. As a result, the systematic review aims to close this significant research gap. Kitchenham and Brereton [2] recommendations were selected to evaluate and explain all homomorphic encryption research questions. Our work is motivated by the revolutionary work of Craig Gentry [3,4]. Additionally, the fact that fully homomorphic encryption will act as a boon to the healthcare industry as it will preserve complete privacy of patient health data is also a path of motivation. Reviewing the processes outlined in Fig. 2 will give a basic understanding of the systematic review process:

- ***Define research/review question:*** After reading various research/Journal articles and magazines and consulting with the expertise in the area of homomorphic encryption. Various research questions were identified.
- ***Develop Review Protocol:*** Pre-define the kind of research that will be included, as well as the procedures for collecting, evaluating, and analysing data.
- ***Identification of Research:*** After, Gentry's revolutionary work in homomorphic encryption, a number of homomorphic encryption methodologies in healthcare and bioinformatics were published. Despite tremendous research in homomorphic encryption there is no systematic review that considers quality of research and development.
- ***Extraction:*** Relevant research articles were included and irrelevant were excluded.
- ***Study Quality Assessment:*** Research articles were selected from popular repositories with keywords as homomorphic encryption to review basic homomorphic approaches.
- ***Data Synthesis:*** This phase entailed presenting data in descriptive and graphical form. It will help to make the overall evaluation of outcomes easier.
- ***Knowledge Translation:*** The findings and details of the review will be distributed to relevant target groups in a variety of media.

Review planning

The accomplishment behind each review depends on the selection of good-quality papers with unique work and genuine references. Thus, recognized journals, conference

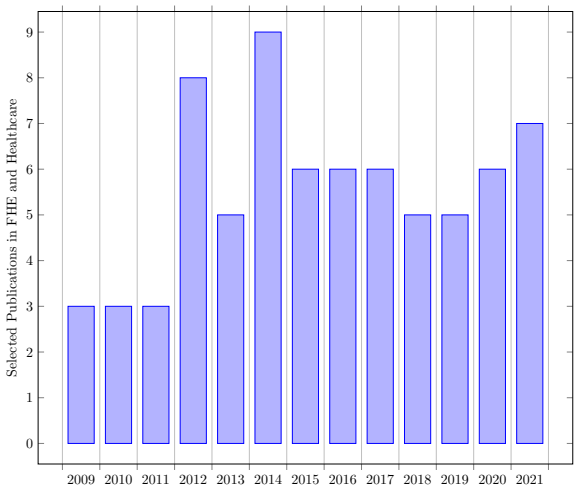

Fig. 3 Scientific Articles from year 2009 to 2021

proceedings, and databases were investigated and explored in the area of homomorphic encryption. Scientific publications from Scopus, ACM Digital library, Springer Link, Sciencedirect, Google Scholar were selected based upon research questions given in Table 1. Fundamental studies in PHE, SWHE that function as cornerstones of homomorphic encryption were chosen first, followed by publications focused only on fully homomorphic encryption. A total of 1815 scientific papers were obtained using a database search with Keywords used for search as 'homomorphic encryption', and 'homomorphic encryption' or "medical" OR "healthcare" OR "bioinformatics" OR "EHR" OR "patient" OR "health" OR "medicine". Following the removal of duplicate documents, a total of 857 records were evaluated for title screening. After screening title total 194 articles were selected for abstract screening. In abstract screening 69 papers that were focused on homomorphic encryption based upon LWE, NTRU, Lattices, Integers, and HE papers focused mainly on healthcare and bioinformatics were selected. Other than that 19 important papers in PHE and SWHE (consider Fig. 4) were chosen for better understanding the concept of homomorphic encryption.

Inclusion and exclusion criteria

Scientific articles in journals, conferences proceedings, workshops published in the year range from Jan 2009 to Dec 2021 (Fig. 3) were considered. Other than that, Partial and Somewhat homomorphic encryption papers of the old era were also included to better understand the concept of homomorphic encryption. All quality research publications of fully homomorphic encryption after the Gentry FHE scheme were considered. Articles that were focused on the applicability of homomorphic encryption other than healthcare or bioinformatics were excluded.

Research questions

Prime objective of this review writing is to categorize the current literature on homomorphic encryption with its contributions in health informatics. This research study's end result is the identification and examination of homomorphic encryption methods in healthcare. A set of research questions are formulated for this systematic literature review in Table 1.

Background

The medical services industry is experiencing a digital revolution. Modernizing medical care has prompted another time of computerized wellbeing and health. Medical services information is gathered from different sources (e.g., sensors associated with patients) and stored in unique medical services clouds (e.g., private and public clouds). Also, the volume of agglomerated medical information is sufficiently enormous to qualify as "Big Data". As cloud medical services become a well-defined component in the medical services industry, there is a more critical requirement for safely sharing patient data across such dissimilar medical services clouds. Besides, with Accountable Treatment Organizations (ACOs) (e.g., medical service providers, specialists, clinics, and protection providers) collaborate to provide top-notch care, with demand for constant availability across cloud medical services higher than at any point in recent times. A disentangled patient-driven paradigm, in which patients can switch suppliers while still providing their data in a useful way for better diagnosis and treatment, and, in the long term, for enhanced global health, is appealing. As of now, medical care suppliers who have delicate patient information in private medical care clouds across the globe are reluctant to share that data on account of security and protection issues. As medical care suppliers move to the local area and public cloud-based administrations, a requirement for a secure connection between divergent medical care cloud increments. Moreover, security guidelines forced by Health Insurance Portability and Accountability Act (HIPAA) [6] and Health Information Technology for Economic and Clinical Health (HITECH) [7] place a cumbersome undertaking on medical care Information Technology (IT) framework to be agreeable with protection and security guidelines. Moreover, with arising Internet of Things (IoT) market and its mix in the vast information cloud stage, there is expanded worry about security and protection with the medical services cloud worldview. Many researchers contributed with their study in homomorphic encryption. Homomorphic encryption has three types: partial homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), and fully homomorphic encryption Fig. 5. PHE supports either