Mesopotamian journal of Cybersecurity
Vol.5,No.3, **pp**. 953–976
DOI: https://doi.org/10.58496/MJCS/2025/054; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Blockchain-Powered Dynamic Segmentation in Personal Health Record

Mishall Al-Zubaidie[1],*, Wid Alaa Jebbar[1],

[1] *Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq.*

ARTICLE INFO

Article history

Received 12 Jun 2025
Revised 24 Jul 2025
Accepted 09 Aug 2025
Published 17 Sep 2025

Keywords

Blockchain technology

DS

FAR

NER

PHR

ABSTRACT

Sensitive patient data must be handled securely in modern oncology care to protect patient privacy, regulatory compliance, and clinical decision-making integrity. Conventional centralized healthcare systems pose serious threats to patient confidentiality and treatment continuity because of their susceptibility to data breaches, illegal access, and single points of failure. This study suggests a blockchain-based decentralized cancer healthcare security solution. The proposed system is based on the idea of layers; each layer has a distinct function that gives it a feature that sets it apart from the others. A hierarchical clustering algorithm (HCA) is used in the first layer to determine the patient's cancer type. The second layer follows, which is mostly founded on the dynamic segmentation (DS) principle. To guarantee high security, patients are isolated on the basis of their kind in various segments. The data are then compressed via the snappy algorithm (SA) at the compression layer. To prevent hacking, the smart contracts layer then applies conditions to each of those segments. These conditions are based on the named entity recognition (NER) algorithm's decision, which is crucial in deciding whether to use blockchain technology (BCT), and ChaCha20 encryption is used to protect the confidentiality of distributed transactions in BCT. Data analysis revealed that, in comparison with earlier methods, the suggested system offers good security, and the high-performance speed of system interaction did not surpass 0.18 ms. Additionally, we were able to acquire a segmentation time of 0.25 ms, a discrimination time of 1.5 ms, and a smart contract verification time of 0.45 ms.

1. INTRODUCTION

A new technology called blockchain is being used to offer innovative solutions in a variety of sectors, including medicine. Hospitals, labs, pharmacies, physicians, and other healthcare providers store and exchange patient data on a blockchain network. Blockchain-based applications are able to detect significant mistakes accurately in the medical field, even those that could be dangerous. It can thereby improve the transparency, security, and efficiency of medical data exchange across the healthcare sector. By using this technology, medical facilities can enhance the analysis of medical data and gain fresh perspectives. A graphical explanation of BCT technology's numerous features, enablers, and unified workflow procedure to support global healthcare is given. The efficiency of healthcare data could be improved by this technique [1]. This approach can lessen concerns about data manipulation in the healthcare sector and allow for a clear data storage pattern at the highest level of security. It provides data access authentication, flexibility, responsibility, and connectivity. For several reasons, health records need to be kept secure and confidential. BCT helps with the decentralized protection of medical data and avoids certain threats [2]. BCT in connection with medical records is a topic that healthcare institutions are always researching, testing, and learning about [3]. This approach has been shown to be an essential tool in healthcare by implementing the same regulations as those for medications, improving payment systems, and decentralizing patient health history records [4]. The term BCT has been mentioned frequently through this introduction; therefore, what is BCT [5], what are its most prominent benefits in the health sector, and why is its use essential and necessary? This is what we discuss in the next paragraph.

1.1 Healthcare Sector and Revolutionary Blockchain Technology

Blockchain is a decentralized, publicly accessible digital ledger that records transactions and processes on several computers. BCT is a decentralized peer-to-peer (P2P) network of individual computers, sensors, or nodes that records, preserves, and keeps track of transactional or historical data [6]. This guarantees that no record can be altered in reverse without affecting any blocks that follow. BCT connects the current block to the previous block and verifies it, forming a long chain. After all,

*Corresponding author. Email: mishall_zubaidie@utq.edu.iq

BCT is the name of the record. Because each transaction is publicly recorded and validated, BCT provides a high level of accountability [7, 8]. No one can alter any data entered into the BCT. This is accomplished by demonstrating the authenticity and integrity of the data. By keeping data over networks rather than in a single database, BCT increases stability and highlights how readily it may be abused. This is the best way to save all pertinent documents safely in one location. This technology provides a high level of security wherever it is applied and in any field [9]. Additionally, BCT speeds up the process of looking through a single patient database to find applicants who fit certain trial conditions [10, 11]. The network continuously captures previous and present experiences and enables reliable collaboration because all members communicate and store information. This technology can provide insights into the importance of individualized treatment regimens by integrating several networks. This technique is not restricted to any one industry or use case. Instead, it is a technology that has applications in a number of fields, including healthcare, which is the area of interest in this study. Concerning the electronic health system, Table I lists the components that make up this health system.

TABLE I. DIGITAL HEALTH COMPONENTS

Digital health component	**Description**
Electronic health records	Digital versions of patients' paper charts, which streamline data sharing among healthcare providers and improve care coordination. Facilitates easier access to patient information and enhances clinical decision-making.
Health apps	Applications are designed for various health-related purposes, from mental health support to chronic disease management and nutritional tracking.
Health information technology (HIT)	Includes systems for managing health data, such as data analytics, artificial intelligence, and machine learning to derive insights from large datasets. Helps in predictive analytics, personalized medicine, and population health management.
Mobile health (MHealth)	Involves the use of mobile devices (smartphones, tablets) and apps for health monitoring, disease management, and wellness tracking. Examples include fitness trackers, medication reminders, and health-related applications.
Patient portals	Online resources that let consumers make appointments, get in touch with medical professionals, view their health information, and get their prescriptions filled. It promotes self-management and patient involvement.
Personal health record (PHR)	It is personal health information that is kept up to date by the individual. A PHR can be all-inclusive and act as a single location to store a person's medical records, prescription drugs, allergies, and other pertinent health data. PHRs encourage self-advocacy and well-informed decision-making by enabling people to actively participate in their health management.
Telemedicine	Allows patients and medical professionals to consult remotely by messaging, phone conversations, or video conferences. It improves access to care, particularly for people living in rural or underdeveloped areas.
Telehealth services	Broader than telemedicine, including remote monitoring, health education, and wellness programs delivered through digital platforms.
Wearable devices	Technology such as smart watches and fitness trackers that monitor health metrics like heart rate, sleep patterns, and physical activity. Useful for both preventive health and chronic disease management.

1.2 Necessity of the Blockchain in Providing Security for the Digital Health Sector

Digital health refers to the use of digital technologies to enhance health outcomes, expedite healthcare delivery, and empower individuals to take charge of their own health. It includes a broad range of devices, programs, and services that make use of digital resources to improve well-being and health [12]. The digital health sector, in particular, is considered one of the sectors of utmost importance when we discuss the subject of continuous development and modernization of systems in people's daily lives. The necessity of development arises at astonishing speeds. Modern healthcare facilities that are backed by innovations in technology are essential. In this situation, BCT technology is crucial for transforming the medical field [13]. In addition, the landscape of the health system is changing in the direction of a patient-centered approach that places emphasis on two essential components: consistently available services and sufficient medical resources. Healthcare firms can more easily provide appropriate patient care and high-quality medical facilities according to BCT [14]. Using this technology, the laborious and repeated procedure of exchanging health information, which raises expenses for the healthcare sector, can be swiftly resolved. Citizens may participate in health research programs by using BCT technology.

Data interaction, security, integrity, interoperability, and real-time updating and access are all enhanced by this technology. Another significant issue is data security, especially in relation to wearable and customized medicine. The requirement for easy, secure methods for patients and healthcare providers to collect, transmit, and consult data across networks without worrying about security lapses is met by BCT technology. Furthermore, BCT is transparent and private, hiding a person's identity behind complex and secure algorithms that can safeguard private medical information [15]. Physicians, patients, and healthcare providers may securely and swiftly share the same information because of the technology's decentralized nature.

BCT is becoming increasingly popular in the healthcare industry [16]. The comprehensive plan of BCT to revolutionize the healthcare industry in the coming years will involve resolving issues with the current framework. This makes it easier for doctors, patients, and pharmacists to access all the information at any time. BCT technology in connection with medical records is a topic that healthcare institutions are always researching, testing, and learning about [17]. This approach has been shown to be an essential tool in healthcare by implementing the same regulations as those for medications, improving payment systems, and decentralizing patient health history records [18]. In addition to advanced technology such as machine learning and artificial intelligence, BCT is essential to the medical sector [19]. As indicated in Figure 1:

- BCT makes it possible to store and retrieve data securely, preventing errors or ambiguities, facilitating quicker diagnosis, and improving patient care significantly as a result.
- BCT offers a solitary encrypted safe digital platform for data storage and sharing.
- These electronic medical records are instantly accessible and shareable globally, and patients can review them with the convenience of their own homes.
- BCT helps track pharmaceutical supplies and permits their safe arrival.
- The identification of transmission parameters can also be helpful in the real-time reporting of diseases and the analysis of outbreak patterns.
- Owing to BCT's ability to store data in a single ledger, duplicating is virtually impossible. Additionally, several keys can access patient details and are not dependent on a single key.

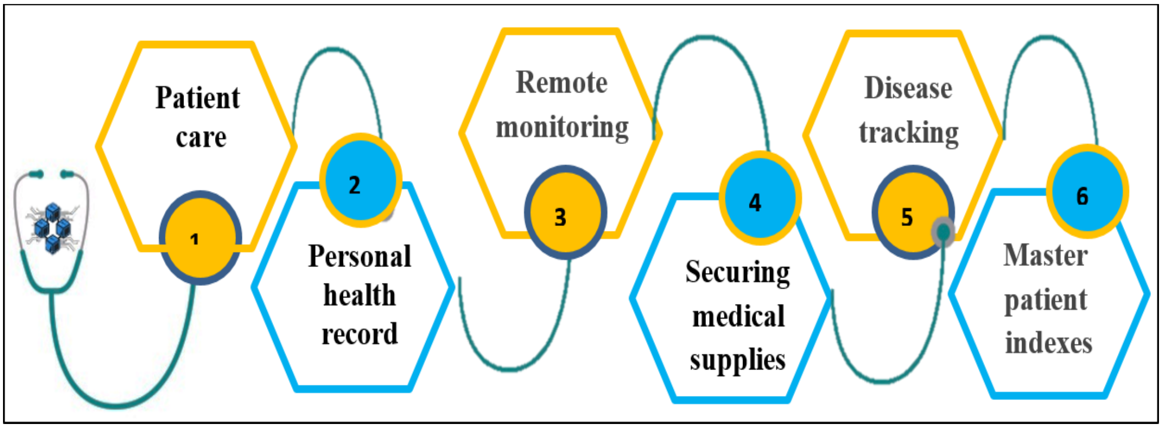


Fig. 1. Blockchain providing healthcare.

1.3 Cancer in Brief

Because our system is a security system that focuses on cancer patients, we must provide a brief overview of this disease, its characteristics, and how our system works in principle can be identified.

Cancer is a group of diseases characterized by the uncontrolled growth and spread of abnormal cells in the body. These cells can invade nearby tissues and, in some cases, spread to other parts of the body through the blood and lymphatic systems, a process known as metastasis. There are many different types of cancer, each classified on the basis of the type of cell or tissue where it originates, such as breast cancer, lung cancer, or leukemia. While the exact cause of cancer can vary, risk factors include genetic predispositions; lifestyle choices, such as smoking or diet; exposure to certain chemicals or radiation; and viral infections. Advances in early detection; treatment options such as surgery, chemotherapy, radiation, and immunotherapy; and research have improved survival rates, but cancer remains a major global health challenge for several reasons [20]. First, it is a complex and diverse set of diseases, with over 100 different types, each requiring different treatment approaches. This complexity makes both early detection and treatment difficult. Many cancers are diagnosed at later stages, when they are more difficult to treat or have already spread, leading to lower survival rates. Additionally, the risk factors for cancer—such as genetics, aging, environmental exposures, and lifestyle habits—are often interconnected and not easily preventable. As populations age, cancer incidence is expected to rise, further straining healthcare systems worldwide. Limited access to healthcare, especially in low- and middle-income countries, can also delay diagnosis and treatment, contributing to worse outcomes.

Creating a PHR system to detect cancer is increasingly considered an important step in addressing these challenges. Early detection significantly improves the chances of successful treatment, and digital tools, such as artificial intelligence (AI), telemedicine, and digital imaging, can help identify cancer at earlier stages, even before symptoms appear [21]. AI, for example, can analyze medical images, such as mammograms or computed tomography (CT) scans, with remarkable accuracy, often identifying tumors that human radiologists might miss. Digital platforms can also enable remote consultations, broadening access to specialist care, particularly in underserved regions. Additionally, digital tools can facilitate better patient monitoring, improving personalized treatment plans and ongoing care. In summary, a well-integrated PHR system could not only aid in earlier cancer detection but also improve accessibility, reduce delays in treatment, and ultimately contribute to better outcomes. Therefore, we focused the study on this particular disease and also emphasized the use of sensors in early treatment. Sending data from sensors to a digital healthcare system can play a crucial role in improving cancer detection, monitoring, and overall patient care. Next, is how using sensors can help:

- **Early detection and continuous monitoring**: Sensors that collect data from patients, such as wearable devices that monitor heart rate, temperature, and blood pressure, or specialized devices that track biomarker levels, can provide continuous streams of real-time data. These data can be sent to a digital healthcare system where they can be analyzed for early signs of abnormal patterns or potential cancer-related changes. For example, wearable sensors might detect unusual changes in a patient's physiology, such as abnormal blood oxygen levels, body temperature, or even irregularities in cell metabolism, which could hint at the presence of cancer. Smartphone apps and devices that track activity levels or detect changes in bodily functions (e.g., skin temperature) can help spot early symptoms of cancer before they become noticeable to the patient [22].

- **Remote patient monitoring and access to specialist care:** In areas where access to healthcare facilities is limited or where specialized care is not easily available, sending sensor data to a centralized digital system can provide patients with remote monitoring. Doctors and oncologists can access these data remotely, allowing them to make timely decisions, adjust treatment plans, and intervene early. For cancer patients undergoing chemotherapy, for example, continuous monitoring of vital signs via sensors can help detect complications like infections or side effects, enabling more rapid intervention [23].

- **Personalized care:** Sensors can also provide valuable information about how a patient's body is responding to cancer treatment, such as chemotherapy or radiation. This real-time feedback allows for more personalized medicine, as treatments can be adjusted based on the data collected. If a patient's sensors indicate an adverse reaction or if their condition worsens, adjustments can be made promptly to avoid complications and improve overall outcomes [24].

- **Early intervention in high-risk groups:** For patients who are at higher risk for cancer due to factors like family history, lifestyle choices, or genetic predispositions, using sensors to monitor their health can lead to earlier intervention. Digital healthcare systems can track changes over time and flag patients for additional screenings or preventative measures when necessary.

- **Improved data integration and collaboration:** Sensor data can be integrated into a broader PHR system, providing a more comprehensive view of a patient's health history and current condition. This integration fosters better communication and collaboration among healthcare providers, enabling a more coordinated approach to cancer care [25].

In this work, we attempt to employ this technology combined with many other technologies and algorithms that will be discussed successively for the purpose of providing high security for the electronic health system. However, the main goal of our research is to employ blockchain technology combined with many other technologies and algorithms that will be discussed successively for the purpose of providing high security for the e-health system. Therefore, the main contributions can be summarized in the following five points:

- Using the dynamic segmentation principle for the first time in a digital healthcare system that is based on a blockchain environment, which is of great importance in isolating data from each other according to the characteristics of the cancer type, thus reducing the exposure of the entire system to hacking, if it happens, since the data are isolated.

- By integrating dynamic segmentation into our proposed system while minimizing the size of the segments via a lightweight algorithm such as snappy, which is very fast and efficient, to the best of our knowledge, this is the first time such a PHR system has been developed.

- The level of security in the suggested system can be increased by using smart contracts (after the NER decision is implemented) to prevent the transfer of any information without fulfilling the terms of the contract and DS technology with distributed BCT to isolate patients and their records from one another. To the best of our knowledge, this is the first time that DS with BCT has been used.

- Focusing on producing a system that addresses security issues with the same importance as generating a system that addresses speed and efficiency in data processing by using lightweight algorithms, whether to verify the terms of the contracts or to reduce the size of the data via compression algorithms (SAs), allows system integration by optimizing the system's performance while maintaining the high level of security it offers.
- Finally, the proposed system works as a diagnostic system with the same efficiency as a security system by relying on technologies distributed over five stages, with each stage providing a specific feature. The first stage is detection, followed by isolation with different segments, reduction in size to maintain efficiency, verification via smart contracts, and storage in the blockchain controlled by the encryption of ChaCha20. Consequently, the proposed system offers diagnosis and verification, reduces system resources, and ensures that high levels of security are combined.

This paper's content is as follows: Previously, we discussed the components of the electronic health system and BCT technology in general, and we discussed the importance of BCT in providing security for health systems (Section 1). In Section 2, we summarize the related works on digital health system techniques. Section 3 describes the mechanism of the proposed personal health record system and how it works. Additionally, in this section, we summarize the methods and their integration together in the proposed security system in detail. On the other hand, Section 4 presents the security analysis against several well-known assaults via the Tamarin Prover analysis tool. The performance evaluation is summarized in Section 5. Section 6 presents the conclusions of the study.

2. RELATED WORK

In this section, we will refer to the most important previous studies that discuss digital health systems that employ BCT and what their strengths and weaknesses are.

Abu-Elezz et al. [1] distinguished the importance and characteristics of adding BCT to the health sector, but at the same time, a theoretical study such as theirs, which reviews the effective role of BCT, must be accompanied by comparisons with systems that do not use BCT, with the creation of numerical tables and analyses that clarify the effective role of this technology. Therefore, this research is considered purely theoretical, has no practical connection, and lacks comparisons. Oladele et al. [8] suggested a BCT-based electronic health data system to safely transfer medical records. The proposal's primary objective is to resolve issues with patient record permit transfers while also improving the accessibility, portability, security, confidentiality, and availability of medical data. However, this study contains a lack of scalability, privacy, and security issues. Ali et al. [14] blended holomorphic encryption methods with BCT technology to propose a fresh approach to enhancing privacy security in Internet of Things-based healthcare applications. By allowing computations on encrypted data without requiring decryption, holomorphic encryption safeguards the privacy of the data while it is being processed. By creating an audit record of every data transaction, the technology increases openness and accountability. Considering variables such as communication cost, transaction volume, and security, researchers have offered a comparison with typical models. While they claim that their proposed system is secure, we do not find any charts showing the percentage of this security or any analysis of it using any security analysis tool, which makes their words unsupported by evidence.

Reegu et al. [26] provided a BCT-based electronic health record (EHR) framework that is compatible with various national and international EHR standards, such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Level Seven (HL7). Research on the most recent developments in the field of electronic health records, particularly those based on BCT, is needed. The study reviewed many national and international EHR standards, identified interoperability issues with existing BCT-based EHR frameworks, and then outlined the standard-based interoperability criteria. In addition to providing the properties of immutability, security, and user control over stored records, the proposed framework can provide the healthcare industry with safer methods of exchanging health information without the need for centralized storage. Their analyses of all their parameters are theoretical analyses, not supported by evidence. In addition, we did not find even one table comparing previous research measures with numbers that support their theory of exchanging data in complete confidentiality or preserving data from manipulation. Chen et al. [27] created a cloud-based and BCT-based storage strategy to manage private medical information. Additionally, a service mechanism for sharing medical records is described. Furthermore, the characteristics of medical BCT are examined and demonstrated through a comparison with traditional systems. On the other hand, it seems that this system is completely dependent on the features of BCT only as a proposed tool, while we notice the absence of other technologies to integrate with blockchain in this proposed system. Sammeta and Parthiban [28] developed a deep learning (DL)-based diagnosis model for safe medical data management supported by the hyperledger blockchain (HBESDM-DLD). Different phases of activities, including encryption, optimal key generation, safe data management based on hyperledger BCT, and diagnosis, are included in the model that is being presented. The model that is being described enables the user to manage data access, provide hospital authorities with the ability to read and write data, and notify emergency contacts. However, this system lacks a comprehensive security analysis supported by a comprehensive performance analysis. Ibor et al. [29] focused on the issues that arise when medical records in a healthcare system are not secure or private. It aimed to close the gap between the encryption algorithms that ought to be employed and the security standards that are currently in use for the management of health information. Conventional databases have traditionally been used in the development of current health information systems. In this proposal, there is no comprehensive analysis of the intention, but there was a comprehensive analysis of the performance, but the security analysis is almost negligible; therefore, this contradicts what was mentioned in their conclusions about their high-security system.

Ismail et al. [30] proposed a lightweight BCT architecture for healthcare data management, reducing computational and communication overhead, using a canal for secure transactions, and avoiding forking, unlike Bitcoin's prevalent approach. However, their proposed system largely lacks comprehensive numerical analysis and performance analysis, which does not provide a complete view of a system that addresses very sensitive data, such as patient data. Ojugo and Otakore [31] used data-mining tools to improve the early detection of gestational diabetes in the Niger Delta. Factors such as age, body mass index, family ties, and environmental conditions increase its likelihood. The main goal of their system is to detect diabetes early and its consequences, but analyzing the speed of their system and the speed of response to the entered data is almost as important and necessary as early detection of the disease because generating a fast system is what leads to an effective system, which is what this research lacks. Rehman et al. [32] built a secure health monitoring system in healthcare 5.0 that allows doctors to monitor patients via medical sensors and take periodic corrective action by forecasting diseases through the use of BCT technology and an intrusion detection system (IDS). According to the analysis of their system, they calculated the effectiveness of their system at 93% in terms of disease diagnosis and prediction, whereas there are many studies with a higher percentage than theirs, which is what this study suffers from.

3. THE PROPOSED PERSONAL HEALTH RECORD SYSTEM AND THE USED METHODS

The purpose of the proposed system is to provide a secure environment for all patients' data from the dangers of manipulation, loss, or hacking and at the same time to diagnose patients with different types of cancer and isolate them from each other. The proposed system consists of the following layers (Figure 2):

- Detection and recognition layer.
- Segmentation and isolation layer.
- Reduction and compression layers.
- Conditions and control layer.
- Verification and storage layer.

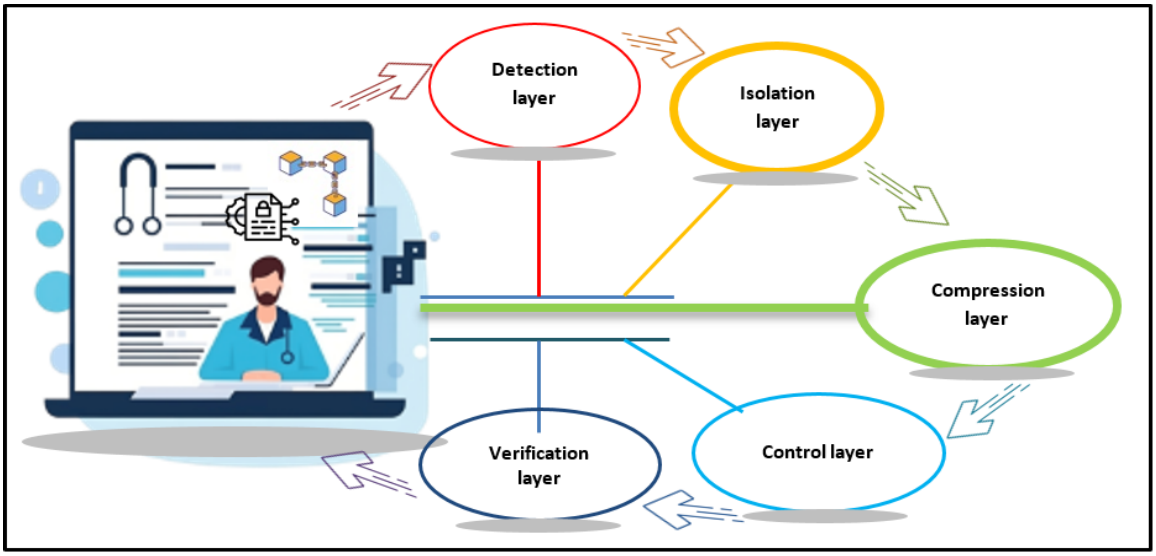


Fig. 2. Overview of the proposed digital system layers.

The detection of the cancer type and diagnosis layer in the proposed system is based on HCA, the isolation phase, and separating each patient according to the type of cancer he/she suffers from into different segments on the basis of what is known as DS technology. Each of these segments consists of what are known as PHRs. These are electronic copies of the paper charts that are kept at a doctor's office. PHRs allow healthcare providers to handle patient data more effectively by storing patients' medical and treatment histories. We developed an integration between the PHRs and the continuity of care record (CCR) systems in this layer, which we will explore in greater depth in the parts that follow. The SA will then be used to compress all of these segments to minimize their size and guarantee that the system's capacity is unaffected by the amount of data. Each of these segments will have its own rules determined to prevent tampering with it, except when certain conditions are met via the principle of smart contracts. The method for determining whether these conditions are met in the proposed system is based on the results of the NER algorithm.

3.1 Methods Used

Each of the technologies that the proposed system relies on is detailed in this section, which simulates the tools that were relied upon in the system, as shown in Figure 3.

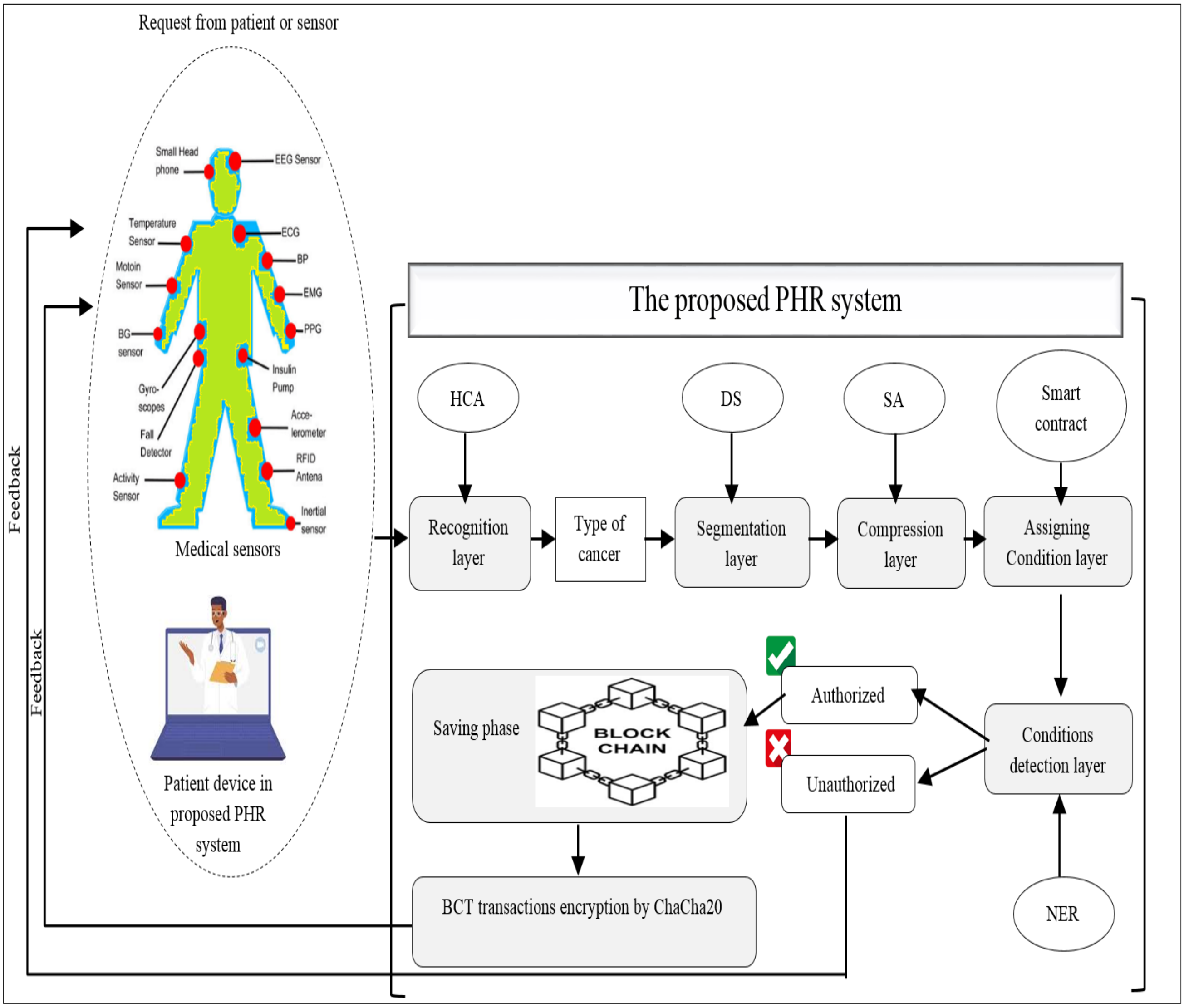


Fig. 3. Detailed hierarchy of the proposed PHR system.

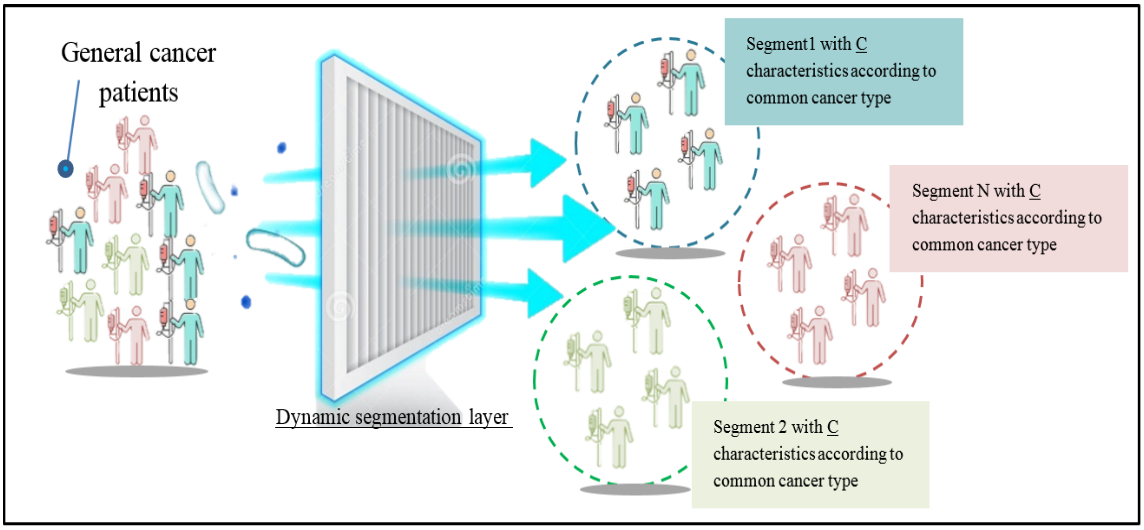

General cancer patients
Dynamic segmentation layer
Segment1 with C characteristics according to common cancer type
Segment N with C characteristics according to common cancer type
Segment 2 with C characteristics according to common cancer type

Fig. 4. Detailed overview of the segmentation layer.

3.1.1 Maintaining the Integrity of the Specifications

The goal of this cluster analysis method is to establish a hierarchy of clusters. Because it does not require a set number of clusters, it is particularly useful for exploratory data analysis. Hierarchical clustering types, Agglomerative (Bottom-Up): Each data point is initially a separate cluster. It combines the two nearest clusters iteratively until the appropriate number of clusters is reached or until all the points are in a single cluster. Divisive (top-down approach): All the data points are first grouped into a single cluster. It divides the cluster into smaller clusters iteratively until either the target number of clusters is reached or every point is in its own cluster. HCA is a helpful technique for classifying cancer types and analyzing cancer-related data. In this case, it can be applied as follows:

- **Data collection**: Relevant data, such as gene expression profiles, methylation patterns, or proteomics data from cancer and normal samples, were obtained.
- **Preprocessing**: Normalize the data to ensure that differences in scale do not affect the clustering results.
- **Distance calculation**: Calculate the distance or similarity between samples (or features) via appropriate metrics (e.g., Euclidean distance, correlation).
- **Clustering**: HCA is applied via an agglomerative approach and a suitable linkage method (e.g., average linkage, Ward’s method).
- **Dendrogram visualization**: Create a dendrogram to visualize the clustering results. This helps identify distinct clusters that may represent different cancer types or subtypes.
- **Interpretation**: Analyze the clusters to identify common characteristics, such as shared gene expression, clinical features, and treatment responses, and validate findings with clinical data or other biological assays.

3.1.2 Dynamic Segmentation

The process of segmenting a database or generic dataset into several groups (or segments) according to needs, interests, traits, and other factors is known as DS. In contrast to depending only on fixed criteria, DS improves flexibility and reactivity by taking into account continuous changes. This revolutionary technique of dividing data into unique segments with characteristics that bring them together, separating them, and distinguishing them from the rest of the segments has been proposed for use for the first time in the proposed system, as shown in Figure 4, because it provides the possibility of isolating patients with similar symptoms together, as shown in Algorithm 1, which helps in diagnosing what they are suffering from easily and facilitating examinations or conducting real-time applications since they are isolated from each other. The use of this technology in the health sector involves the following characteristics: **Patient management**: Medical professionals can divide patient populations according to current health information, including laboratory results, medication compliance, and essential signs. This makes it possible to create customized treatment plans that can vary with patient health.

Risk stratification: By continuously assessing a patient’s health status, a DS can assist in identifying high-risk individuals and enable preventative actions and individualized care plans. **Resource Allocation**: By keeping an eye on patient flow and modifying staffing and equipment in accordance with actual demands, hospitals can employ DSs to distribute resources efficiently. **Population health management**: Healthcare companies can detect patterns and new health concerns by dynamically segmenting their populations. This enables them to promptly implement public health initiatives. **Personalized communication**: By grouping patients according to their communication requirements, preferences, and degrees of involvement, providers can make outreach and education initiatives more successful. Implicitly within this layer, we use the following medical records to ensure the smooth flow of work and the proper transfer and integration of patient information in the system. **Personal health records**: These are electronic copies of the paper charts that are kept at a doctor's office. PHRs are used by healthcare providers to handle patient information more effectively. They contain the medical and treatment history of patients within a practice. We focused on using it in the proposed system for the following reasons: PHRs store comprehensive patient data, including medical history, diagnoses, medications, treatment plans, and immunization records. Healthcare providers can access patient records quickly, which enhances the speed and quality of care. Additionally, these records facilitate communication among different healthcare providers, improving coordination for patients receiving care from multiple specialists. PHRs can be used for reporting and analyzing patient data to improve healthcare outcomes and support quality improvement initiatives. It helps ensure that coding and claims are accurate. The important part of this type of medical record is what is known as a CCR. It is a standardized document that contains essential health information about a patient, designed to facilitate the sharing of medical information among different healthcare providers. The CCR aims to ensure that all members of a patient's care team have access to relevant data, promoting coordinated care and improving patient outcomes. The main components of each patient record displayed in Figure 5, which are isolated and separated from each other by separate segments in the proposed system, are:

- Basic information such as name, date of birth, and contact details was obtained.
- Summary of past medical conditions, surgeries, and treatments.
- Current medications, including dosages and frequency.
- Known allergies to medications or substances.
- Active medical issues that require ongoing management.
- Contact details for the healthcare providers involved in patient care.
- Recommendations for ongoing treatment and follow-up.

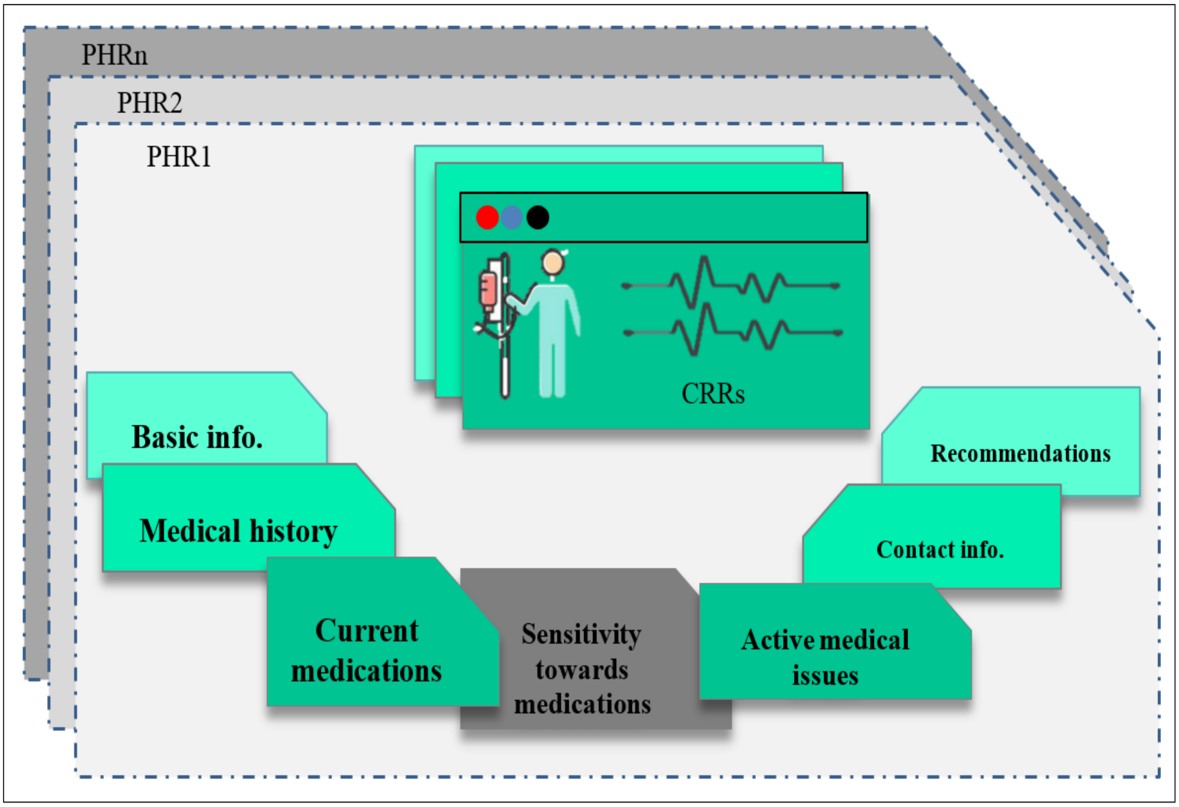


Fig. 5. Patients record components in the proposed system.

3.1.3 Snappy Algorithm

Before proceeding to control the isolated segments, we added a pivotal step to increase the performance of the proposed system by reducing the size of the data that are present in those segments, and this was done by using the SA data compression algorithm. The SA is a fast and efficient algorithm used for data compression, designed to deliver high compression speeds with reasonable trade-offs in terms of compression ratio. It is primarily used for scenarios where speed is critical, such as in real-time applications, databases, and network protocols. SA works by finding patterns in the data and replacing them with shorter representations, typically using techniques like dictionary encoding and sliding windows. Its primary advantage lies in its speed, making it ideal for high-throughput environments where minimizing latency is a priority. PHR systems often address large volumes of medical data (e.g., patient records, medical imaging, diagnostic reports). Figure 6 shows the SA steps. The speed of SA makes it well suited for compressing and transmitting these data over networks, especially in real-time telemedicine or when large datasets are sent between healthcare providers. In summary, SA's ability to provide fast, lightweight compression makes it a good fit for digital healthcare systems, where speed, real-time data handling, and efficient storage are the main reasons why we used and employed this algorithm in the proposed system. The step chunk data involves splitting large datasets, such as a medical image or a large patient record, into smaller chunks or blocks that are suitable for SA. The compression begins by finding repeated patterns within the chunks. Then, the repeated patterns are replaced with shorter codes as dictionary encoding, and finally, the compressed data for each block are output.

Algorithm 1 HCA and DS in the proposed system

```
Begin
Input:
        patientData: List of patient records, where each record contains:
          -     patientID
          -     diagnosis (string)
          -     otherAttributes (dictionary containing additional patient data)
Output:
          -     cancerSegments: Dictionary where keys are cancer types/values are lists of patient records
          -     cancerSegments ← {}

1: Iterate through each patient record in patientData
    FOR each patient in patientData:
         Extract the cancer type from the diagnosis
         cancerType = ExtractCancerType(patient.diagnosis)
         Check if the cancer type is valid and not empty
         IF cancerType IS NOT EMPTY:
              Initialize the list for this cancer type if not already done
         IF cancerType NOT in cancerSegments:
              cancerSegments[cancerType] ← []
        Add the patient record to the corresponding cancer type list
         cancerSegments[cancerType].APPEND(patient)
         Return the dictionary of cancer segments
    RETURN cancerSegments
2: FUNCTION ExtractCancerType(diagnosis):
           -     Helper function to determine the type of cancer from the diagnosis
           -     Input: diagnosis (string)
           -     Output: cancerType (string)
3: Mapping of common cancer diagnoses to types cancerMapping = {
    "lung cancer": "Lung",
    "breast cancer": "Breast",
    "prostate cancer": "Prostate" "skin" Utirine" "Pnceriatic",
    "colorectal cancer": "Colorectal" "Bladder" "Kidney" "Lymphoma",
    }
4: Normalize diagnosis to lower case for matching
             -     normalizedDiagnosis = LOWER(diagnosis)
5: Check each entry in the mapping
     FOR each key, value in cancerMapping:
```

```
     IF normalizedDiagnosis contains key:
    RETURN value # Return the corresponding cancer type
RETURN EMPTY # If no match found
End of algorithm
```

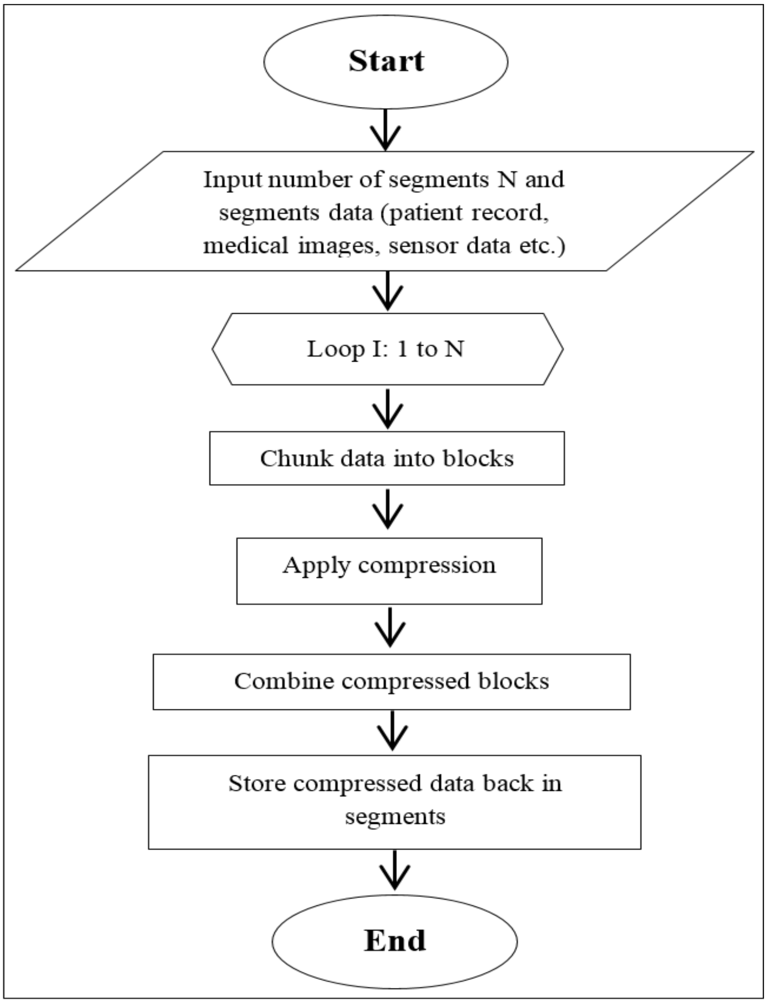

Start
Input number of segments N and segments data (patient record, medical images, sensor data etc.)
Loop I: 1 to N
Chunk data into blocks
Apply compression
Combine compressed blocks
Store compressed data back in segments
End

Fig. 6. SA steps.

3.1.4 Smart Contracts and Named Entity Recognition

After the DS technology has divided and isolated patients into different segments according to the type of cancer, the next step is controlling those segments by setting conditions for transferring, retrieving, or updating data in those segments. The principle of smart contracts has been employed to write the control conditions of the segments in the proposed system. A smart contract is a self-executing contract with the terms of the agreement directly written into the code. It runs on a BCT, which ensures security, transparency, and immutability. In the context of a PHR system, smart contracts can automate and enforce various processes, such as patient consent management, insurance claims processing, and healthcare data sharing. By using smart contracts, healthcare providers can streamline administrative tasks, reduce fraud, and ensure compliance with regulations. For example, a smart contract could automatically trigger payments from insurers to healthcare providers once a service is delivered, or it could securely share patient medical records between authorized parties, with clear terms governing access and usage. This reduces the need for intermediaries, enhances trust, and improves the overall efficiency of healthcare systems.

In this layer, we have employed the NER algorithm to verify the terms of the smart contract. This algorithm identifies and classifies entities in text, locations, and dates. It helps in extracting structured information from unstructured data, which is essential for tasks like information retrieval and natural language processing. In the case of the proposed system, we managed NER to be used to identify and extract specific conditions and terms from smart contracts, aiding in the analysis and understanding of contract clauses. This can ultimately enhance automated contract management and compliance checks, as shown in Algorithm 2. This helps ensure that conditions for services, payments, and regulations are met in the proposed system. The smart contract is written and focused on matching the identity of the person who entered the data with the identity of the person previously stored in the database to avoid updating or storing the data by untrusted people. It includes:

- **Data input validation**: Extract and validate relevant patient data (such as names and medical terms).
- **Access control**: A smart contract can include authentication checks that only allow verified users to input data on the basis of the roles defined in the contract.
- **Audit logging**: Every data entry can trigger an event in the smart contract that logs the action, timestamp, and user identity.
- **Conditions for data entry**: Conditions for the smart contract that require verified data inputs from NER before allowing data storage on the BCT.

Algorithm 2 NER with smart contract

```
Begin
Input: S ← The isolated segments with the terms of smart contract.
Output: R ← The result of detection
Algorithm: PHR smart contract NER

1: Data preprocessing:
        -   Clean the text:
    Remove unnecessary formatting, and non-relevant content.
    Convert text to lowercase.
2: Tokenization:
        -   For each sentence in the smart_contract_text:
        -   Tokenize the sentence into words (tokens).
        -   Initialize a list ‘tokens[]‘ to store individual tokens.
3: Part-of-speech (POS) tagging and dependency parsing:
        -   Perform POS tagging on each token in the sentence.
        -   Apply dependency parsing to identify grammatical structure and relationships between words.
4: For each sentence or chunk of text:
        -   Use the NER model to extract basic named entities (like names, dates, locations, etc.).
        -   For each entity identified, store the entity text and its corresponding label in ’entities[]’.
5: Domain-specific entity recognition:
        -   Load healthcare domain-specific patterns (e.g., patterns for medical terms, contract terms, etc.).
        -   Define custom rules: Create rules or patterns for healthcare-specific entities (e.g., terms like "patient",
            "provider", "insurance coverage", etc.).
        -   Use a matcher to find these patterns in the tokenized text.
        -   For each pattern match, append the matched entity and its label to ’entities[]’.
6: Resolve cases where multiple entities are identified with similar names or types.
        -   Coreference resolution: Link references (e.g., "the provider" to a named entity "Dr. XXX").
7: Return extracted entities:
        -   For each entity in ‘entities[]’:
        -   Extract entity text and its label (e.g., "patient name" - "cancer type" - "insurance coverage" -
            CONTRACT_TERM).
8: Return the final list of extracted data that matches the terms.
End of algorithm
```

3.1.5 Blockchain with Lightweight Encryption

BCT is extremely suitable for use with the proposed PHR because BCT works on the principle of decentralization, i.e., peer-to-peer data distribution. BCT uses hashing to prevent data alteration in transactions. Healthcare systems can be made far more secure, efficient, and private by combining blockchain technology (for decentralized, unchangeable records) with a lightweight algorithm such as ChaCha20 (for stream encryption). To make patient data in transactions more secure, we combined the blockchain with lightweight encryption algorithms, where in lightweight encryption, algorithms are specifically designed to consume minimal processing power, memory, and energy, making them ideal to use [33–37], where we use ChaCha20 to encrypt transactions and thus provide confidentiality requirements. In the proposed system, we use ChaCha20 with a 256-bit key length and 20 rounds. We adopted this algorithm in our proposal because the healthcare blockchain system that uses ChaCha20 encryption offers a high degree of efficiency, security, and anonymity. The important advantages of this algorithm include the following:

- Strong encryption of patient data guarantees privacy.
- Encryption is scalable and compatible with high-throughput settings.
- Records that are unchangeable, auditable, and have data storage that is impenetrable.
- Key management-based access control for safe decryption and patient confidentiality. Additionally, this algorithm is resistant to various confidentiality attacks.

Figure 7 shows ChaCha20 encryption with BCT blocks in the proposed PHR.

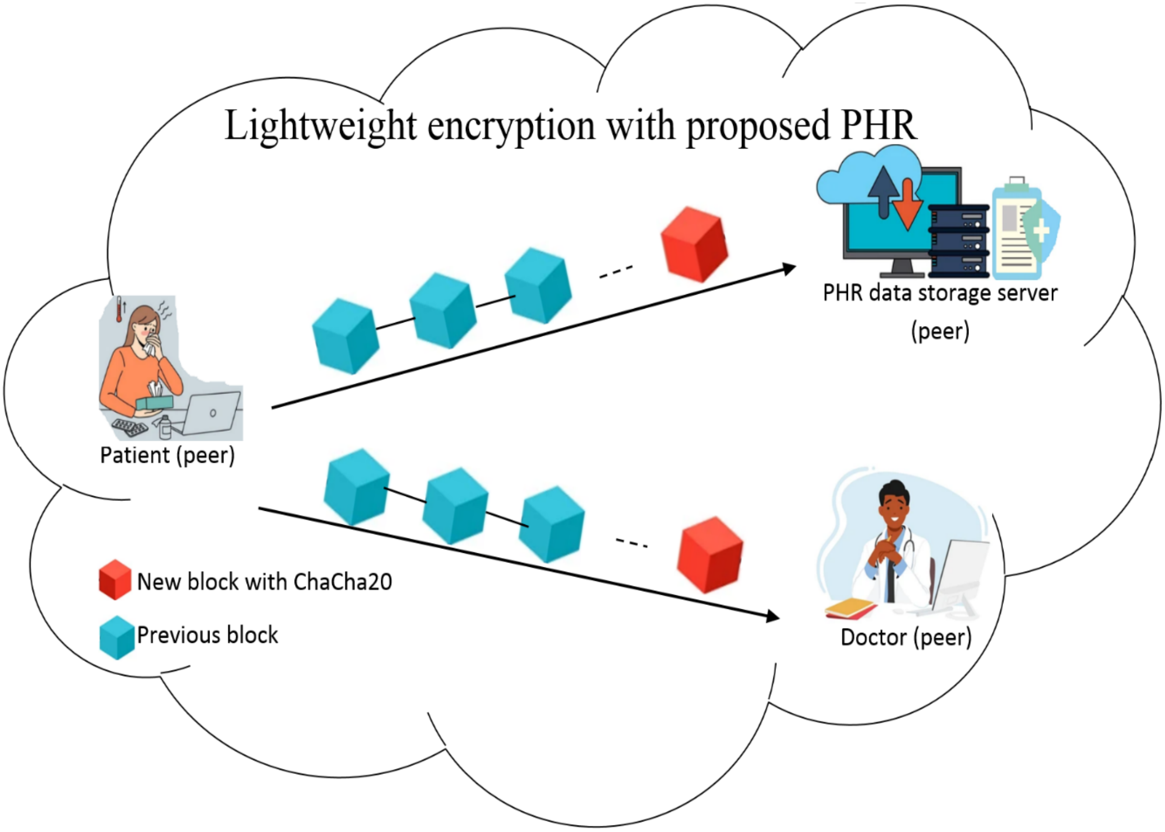


Fig. 7. ChaCha20 encryption for blockchain transactions.

4. SECURITY EXAMINATION OF THE PERSONAL HEALTH RECORD RISKS

This section is divided into two subsections. First, we will theoretically analyze how the proposed PHR system will counter attacks and which techniques will be used for each type. The other section is concerned with exposing the system to a real exchange environment via the Tamarin prover analysis tool to test a set of security features, which will be explained in this section.

4.1 Analysis of Attacks Theoretically

Owing to the sensitive nature of patient data, system security is crucial in PHR systems, where the system's resilience to attacks is deemed crucial. The examination of the threats to the PHR system's security and how the suggested module successfully counters them are then summarized.

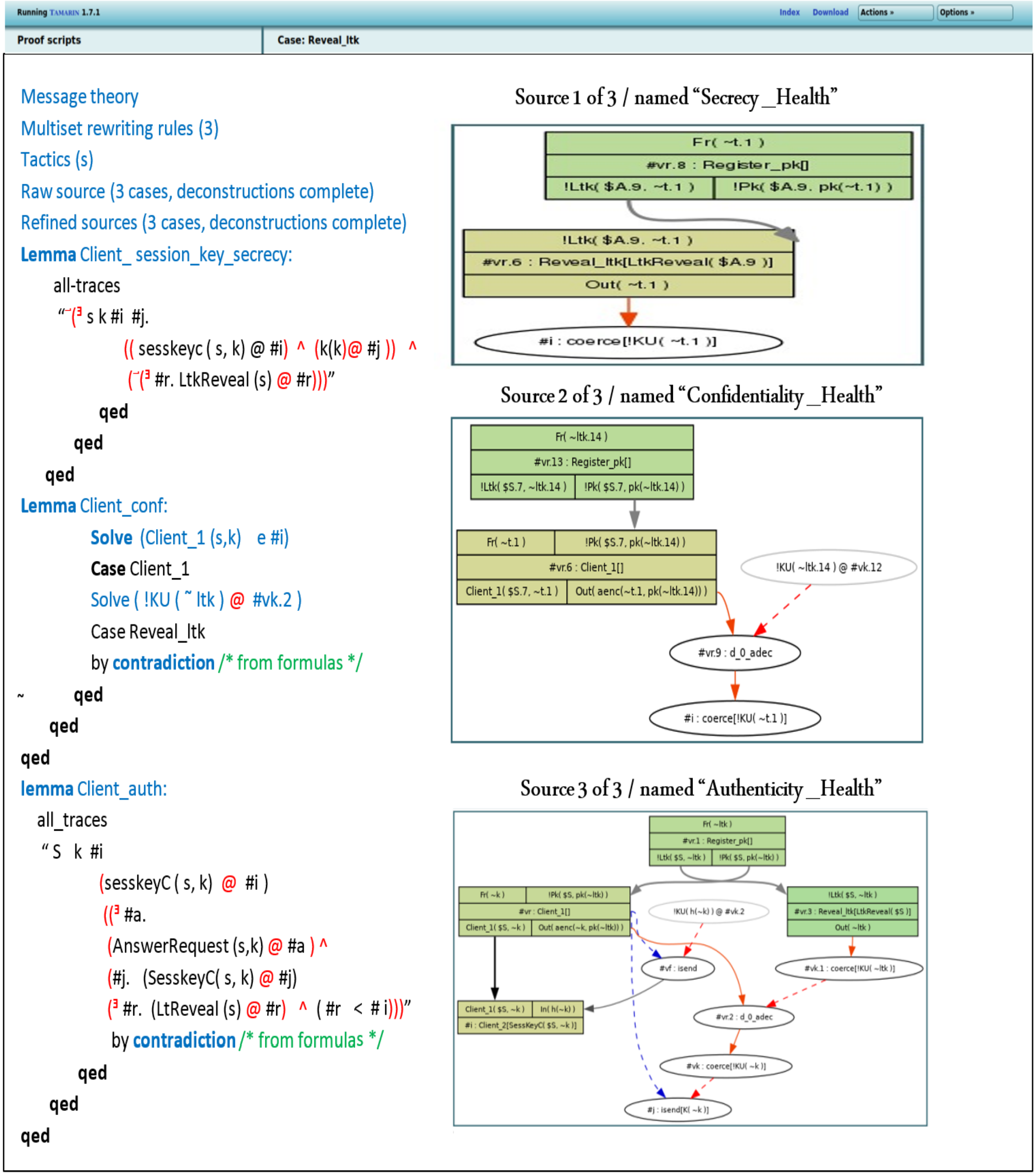
- Ransomware attack: This type of cyberattack in which a victim's files or systems are encrypted by malicious software, rendering them unusable. After that, the attacker requests a ransom, usually in PHR, in return for the decryption key that will allow the data to be accessed again. The following is how this type of assault works: In the phase of encryption, the attacker first encrypts the victim's device or network's files. Second, during the ransom demand phase, victims are notified that they must pay a certain sum to restore access. The last stage is the threat of data loss, during which attackers frequently threaten to erase the data forever if the ransom is not paid within a specific amount of time. This kind of assault is prevented in the suggested system by using smart contracts, which withhold database information until certain requirements are satisfied.

- Insider threat attack: This refers to the dangers posed by employees who possess inside knowledge of a health institution's data, computer systems, and security procedures. These people may be workers, subcontractors, or business associates who carelessly or maliciously abuse their access. For financial gain, retaliation, or personal advantage, some insiders may purposefully steal or damage data. Others may unintentionally expose sensitive information or cause harm due to negligence or lack of awareness. Insiders typically have legitimate access to systems and data, making it easier for them to exploit vulnerabilities. However, in the proposed system, this type of attack is addressed by relying on distributed BCT technology, in which tampering is detected by all people in the network, in addition to the principle of smart contracts.
- Credential stuffing attack: This type of cyberattack hackers access accounts on other services without authorization by using username and password pairs that were obtained in one breach. Since many users reuse the same credentials across multiple websites, this makes them vulnerable. The attackers collect credentials from data breaches and use automated tools to test these combinations against various websites and services. The process is typically automated, allowing attackers to test thousands or even millions of combinations quickly; therefore, many people reuse passwords, and attackers can gain access to numerous accounts even if they have only a small number of valid credentials. In a system that relies on the principle of decentralization by entering data, in addition to the use of the principle of DS and verification of smart contract terms and the absence of reliance on passwords or traditional protection methods, such as the proposed system, this type of attack does not affect it.
- Alternative historical attack: The purpose of this assault is to alter health data and information records to change existing records or create new records. The attacker seeks to fabricate a new account of what happened via archives from the past. If an alternate history attack is successful, it could provide an inaccurate alternate medical history in addition to tampering with or altering crucial and sensitive patient information such as diagnosis, treatment, and medical history found in electronic personal healthcare records. The proposed system counters this attack by using the DS principle, which isolates patient records from each other, in addition to the inability to access the data because it is protected by smart contract conditions.
- Brute force attack: This is a method used by cybercriminals to gain unauthorized access to a system, account, or encrypted data by systematically trying every possible combination of passwords or keys until the correct one is found. The attacker attempts every possible combination, making it a straightforward but time-consuming approach. Also, the attackers often use automated software to speed up the process, allowing them to test thousands or millions of combinations quickly. Brute force attacks are more successful against accounts with weak or commonly used passwords. The proposed system does not rely on this traditional method of entering data, such as the password method; but, on the contrary, it relies on smart contracts enhanced with a verification algorithm, such as NER, which is an easy and fast verification algorithm. Moreover, the proposed system is based on the lightweight and secure ChaCha20 algorithm to protect PHR data and resist brute force attacks.
- Session hijacking attack: This kind of cyberattack is when a hacker assumes control of a user's active online application session, mimicking the real user and gaining unauthorized access to private data or actions. The attacker captures the session ID, which is used to authenticate the user's active session. This can be done through various means, such as stealing cookies or using network sniffing tools. Once the attacker has the session ID, they can impersonate the user without needing to log in with credentials. Session hijacking can be challenging to detect, as it often occurs without any direct interaction with the victim. The suggested system's multiple levels and algorithms for each tier boost protection against these kinds of attacks.

We exposed the proposed system to different types of attacks, including those related to the network, those related to data, those related to methods of accessing data, and those related to engineering methods that are part of the system's structure and construction. This is to ensure the high security provided by the proposed system by confronting different types of attacks.

4.2 System Security Analysis in Practice

A strong and effective tool for formally verifying cryptographic protocols, called Tamarin Prover, that we used to conduct a security analysis of the suggested system. It operates within the symbolic model, providing a strict framework for analyzing the security properties of protocols against various attacks. In this tool, protocols are described in a high-level language that is easy to understand and manipulate. This language allows users to define roles, channels, events, and processes involved in the protocol. Users specify the desired security properties, such as confidentiality, integrity, authentication, non-repudiation, or freshness. These properties are expressed as logical formulas. It provides the result with the usage of symbolic execution and constriction on solving techniques to explore all possible execution paths and identify potential vulnerabilities. If the Tamarin Prover finds a violation of the security property, it generates an attack trace, which outlines the steps an attacker could take to exploit the vulnerability. If the protocol is secure, the Tamarin Prover generates a formal proof of security. As shown in Figure 8, at the end of each of the authenticity, confidentiality, and security properties, there is a “qed”, which means that the security property is verified and that no vulnerabilities are found when Tamarin outputs "qed" to signify that the proof has been successfully completed and that the property holds true for the given protocol.



```
Message theory
Multiset rewriting rules (3)
Tactics (s)
Raw source (3 cases, deconstructions complete)
Refined sources (3 cases, deconstructions complete)
Lemma Client_ session_key_secrecy:
      all-traces
       “¬(∃ s k #i  #j.
                ((sesskeyc ( s, k) @ #i)  ^  (k(k)@ #j ))  ^
                 (¬(∃ #r. LtkReveal (s) @ #r)))”
             qed
          qed
      qed
Lemma Client_conf:
             Solve  (Client_1 (s,k)   e #i)
             Case Client_1
             Solve ( !KU ( ˜ ltk ) @  #vk.2 )
             Case Reveal_ltk
             by contradiction /* from formulas */
~         qed
      qed
qed
lemma Client_auth:
    all_traces
    “ S   k  #i
               (sesskeyC ( s, k)  @  #i )
                ((∃ #a.
                 (AnswerRequest (s,k) @ #a ) ^
                 (#j.   (SesskeyC( s, k) @ #j)
                 (∃ #r.  (LtReveal (s) @ #r)   ^  ( #r   <  # i)))”
                  by contradiction /* from formulas */
          qed
      qed
qed
```

Source 1 of 3 / named “Secrecy_Health”

Source 2 of 3 / named “Confidentiality_Health”

Source 3 of 3 / named “Authenticity_Health”

Fig. 8. Tamarin prover security, authenticity and confidentiality analysis results.

5. PERFORMANCE ANALYSIS OF THE PROPOSED PHR SYSTEM

The performance of the suggested system was constructed via the Java programming language in an integrated development environment called "Eclipse" on the Ubuntu 16.04 LTS system, which is covered in the sections that follow practically. The PC utilized for the study has the characteristics of an Intel Core^{TM} 3110M CPU and 4.00 GB of RAM.

- Speed of reaction factor: The amount of time required for the system to process and evaluate data, such as test results, patient records, or diagnostic inputs, before providing feedback or recommendations; the time required for the system to display results or recognize user actions following a user's interaction with the interface. Also, it refers to the time required for the system to communicate with external services or databases, such as retrieving patient information or interfacing with medical devices. In the proposed system, we analyzed this parameter because of its great importance in determining the effectiveness of the user's experience with the system to show the speed of performance compared with the security it provides.

  In all the performance analysis figures, the x-axis represents the number of executions that we have reexecuted to ensure the most accurate result, whereas the y-axis represents the parameter of interest in the analysis, whether it is speed, percentage, or time. As illustrated in Figures 9, 10, and 11, we find that the time taken is no more than 0.18 ms, which is considered fast compared with previous works and compared with the works that the system accomplishes, such as retrieving data, adding new data, or even modifying it. Figure 12 summarizes and compares the speed of completing all these operations. Table II illustrates the comparison with the previous studies on the speed of reaction parameter. In this table, we note the superiority of the proposed system over other systems that use BCT as a basis for their systems, as we notice that the proposed system only takes 0.18 milliseconds, which is considered a fast rate when compared to other systems.

TABLE II. HEALTHCARE-BASED BCT SYSTEM SPEED OF REACTION VS. THE PROPOSED SYSTEM

Healthcare system with BCT	Speed of reaction
[8] 2024	0.78 second
[29] 2023	10 minutes
[30] 2019	2.5 seconds
[31] 2018	0.4 seconds
Proposed system	0.18 Milliseconds

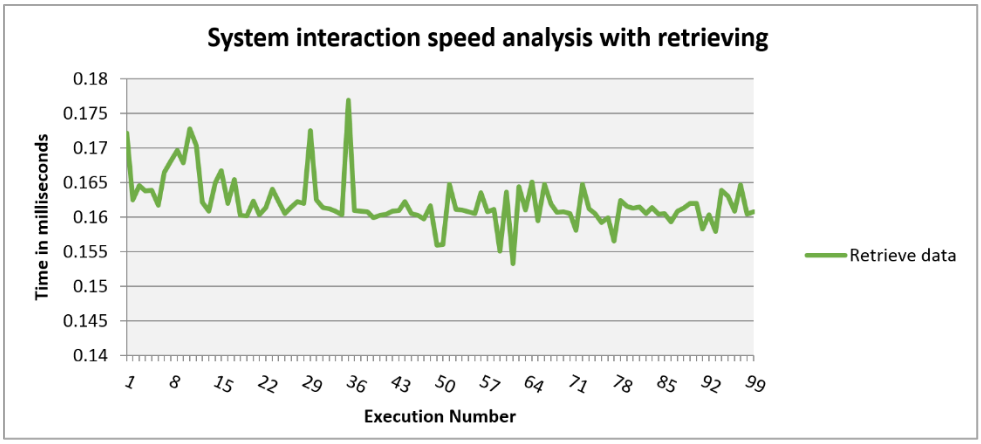


Fig. 9. Query data speed analysis.

- Prediction accuracy factor: This parameter refers to the accuracy or confidence level of a system's predictions regarding patient outcomes, diagnoses, or treatment responses. This indicates how accurately the system can forecast certain health events on the basis of the data stored on the BCT. Table III provides a comparison between the proposed PHR system and existing health systems. For this reason, we consider it an important part of the performance analysis of the proposed system, as shown in Figure 13. As shown in Figure 13, the prediction rate of the proposed system for different types of cancer ranges between 98 and 99, which is considered a high rate for medical systems in general and systems that address cancer in particular.

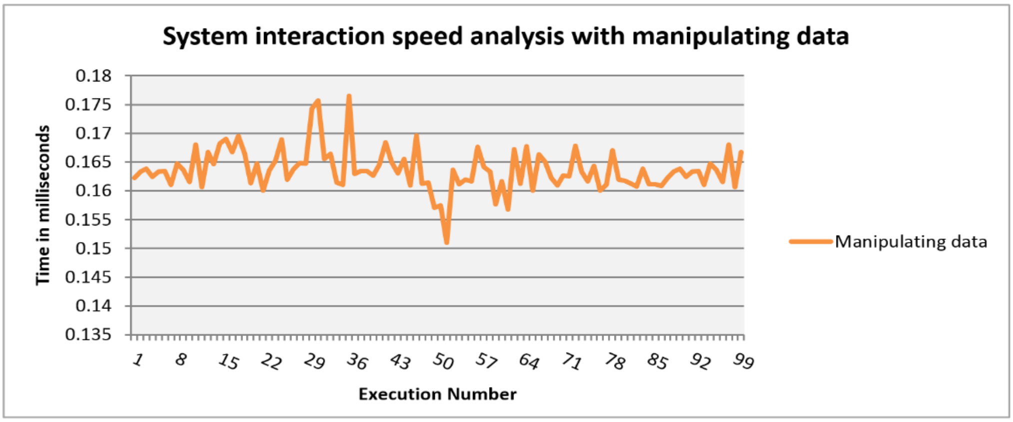


Fig. 10. Update data speed analysis.

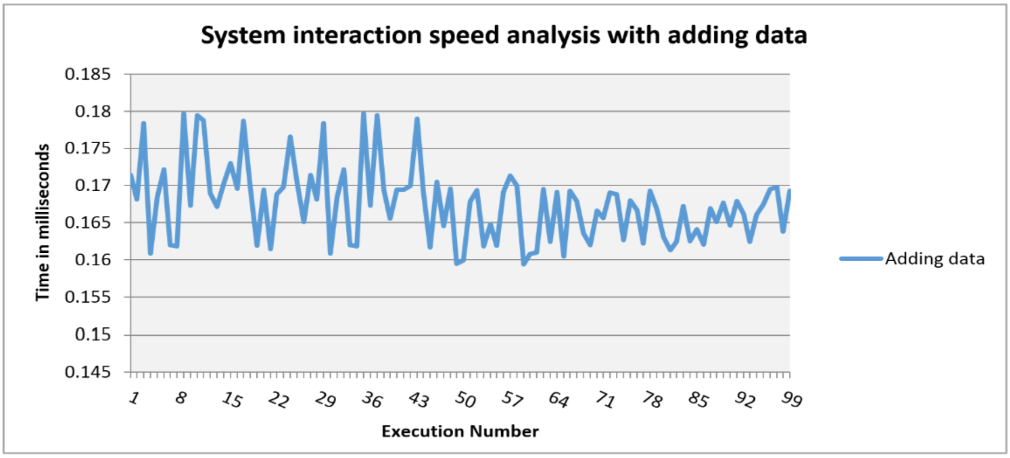


Fig. 11. Adding data speed analysis.

TABLE III. HEALTHCARE-BASED BCT SYSTEM SPEED OF REACTION VS. THE PROPOSED SYSTEM

Healthcare system with BCT	**Prediction percentage**
[31] 2018	90%
[32] 2022	96%
Proposed system	98.7%

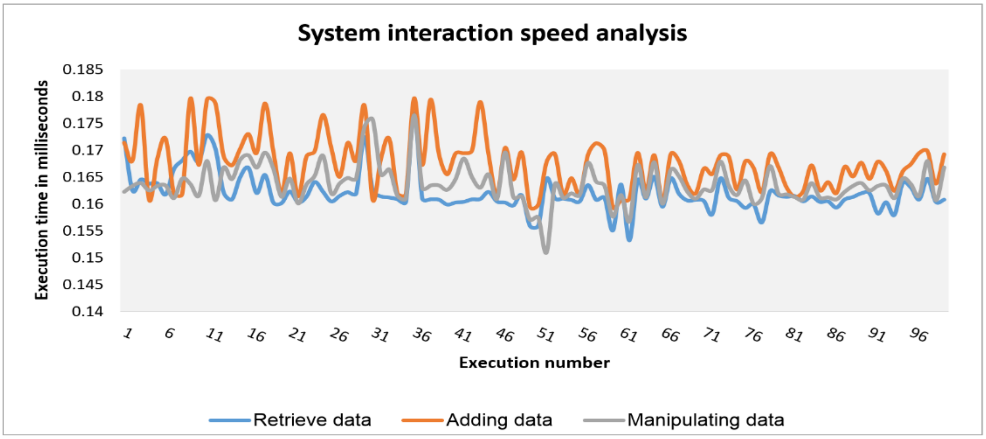


Fig. 12. Comparison of speed analysis.

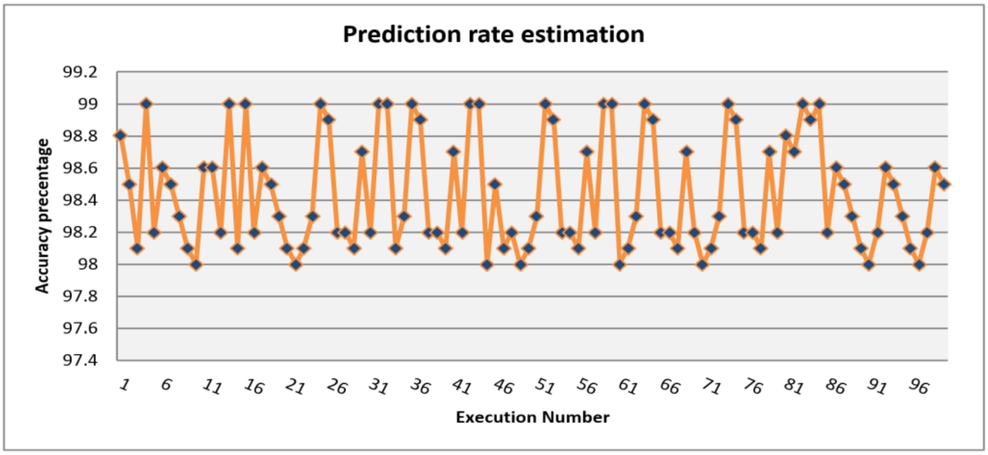


Fig. 13. Proposed system prediction estimation.

- Analysis of the proposed PHR system techniques and algorithms: Here, specifically, we perform a comprehensive analysis of the performance of the proposed algorithms and techniques combined together to work in harmony and balance. We present the performance of each technique used in Figures 14, 15, 16, 17, and 18.

  As we can see from the figures above, the analysis of these algorithms has shown the effectiveness and accuracy of these techniques in contributing to the production of a system that enhances, with its high performance, the security obtained from integrating these techniques with each other. We note that the time it takes for the DS to be isolated according to the type of cancer is not more than 0.25 ms. Additionally, the time of the HCA to be performed is 1.5 ms, whereas the speed it takes for the NER algorithm to detect the conditions is not more than 0.45 ms. Finally, the SA has been evaluated in Figure 16, where the compression ratio is 0.18 and the decompression ratio is 0.21, which is considered high compression and decompression ratios compared with those of other algorithms, especially since we are dealing with a large amount of data such as health system data.

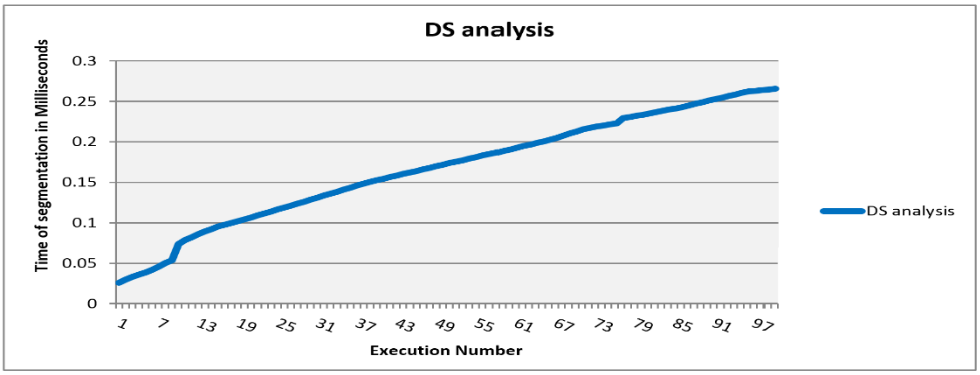


Fig. 14. DS evaluation.

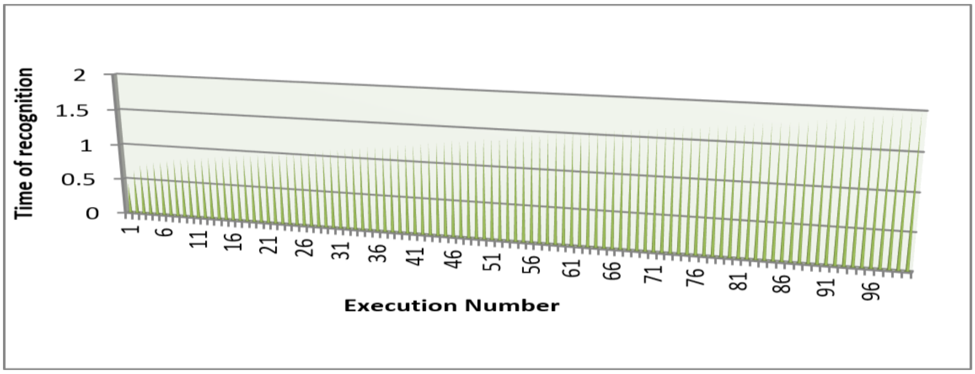


Fig. 15. HCA evaluation.

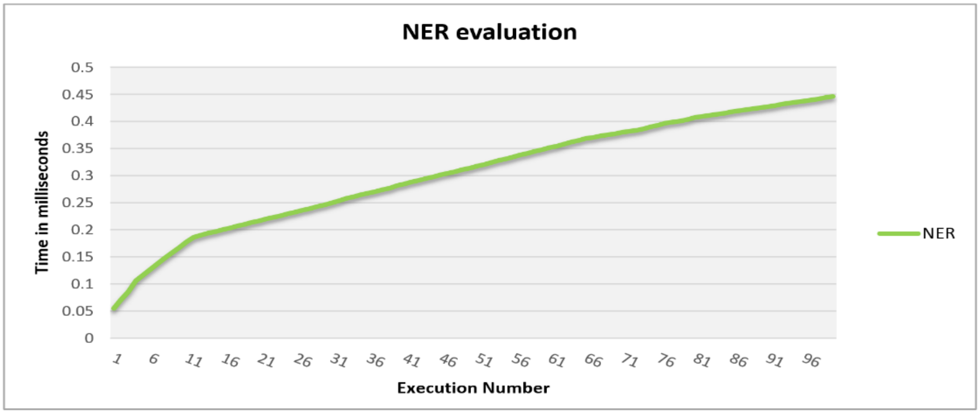


Fig. 16. NER evaluation.

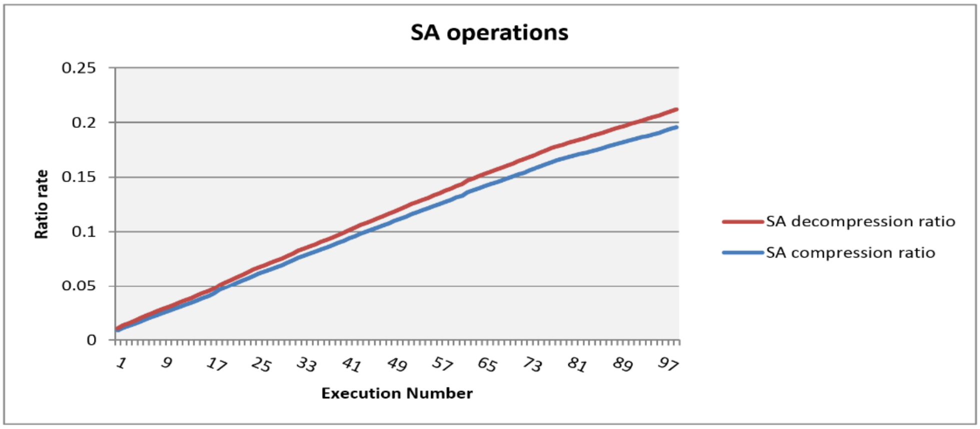


Fig. 17. SA evaluation.

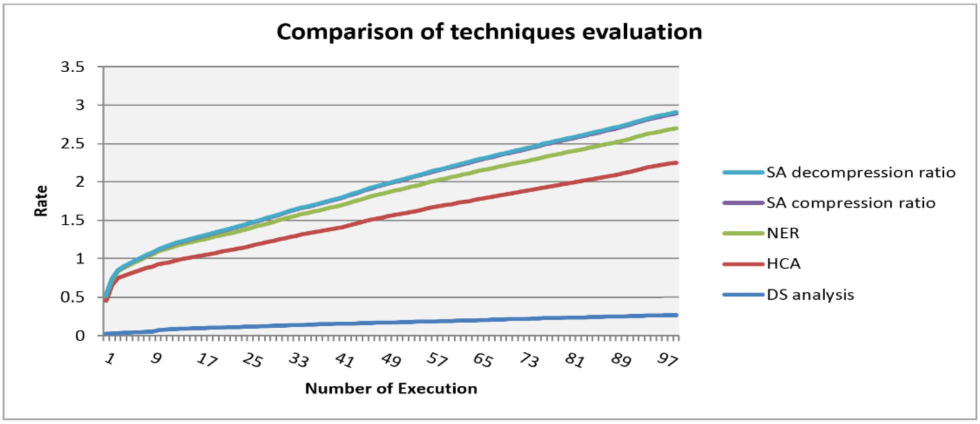


Fig. 18. Full techniques evaluation comparison.

- False acceptance and false rejection rates: Two important performance metrics are used to evaluate the accuracy of a system in verifying or identifying individuals. These terms are particularly relevant in fields such as authentication and recognition. Next is what each term means:

1- **False acceptance rate (FAR)**: This rate refers to the percentage of times the system incorrectly accepts an unauthorized user or an imposter as legitimate, i.e., the system erroneously grants access to someone who should not have access.

$$FAR = \frac{Number\ of\ FalseAccepts}{Number\ of\ FalseAccepts\ +\ Number\ of\ TrueRejects} * 100 \qquad (1)$$

2- **False rejection rate (FRR)**: It is a performance metric used in authentication systems to measure how often the system incorrectly rejects an authorized user. In other words, it is the percentage of times a legitimate user is denied access or wrongly identified as an imposter.

$$FRR = \frac{Number\ of\ FalseRejections}{Number\ of\ TrueAccepts\ +\ Number\ of\ FalseRe\ jects} * 100 \qquad (2)$$

As we can see from Figures 19 and 20, the percentage of the proposed system is considered low when compared to the previous systems in Table IV.

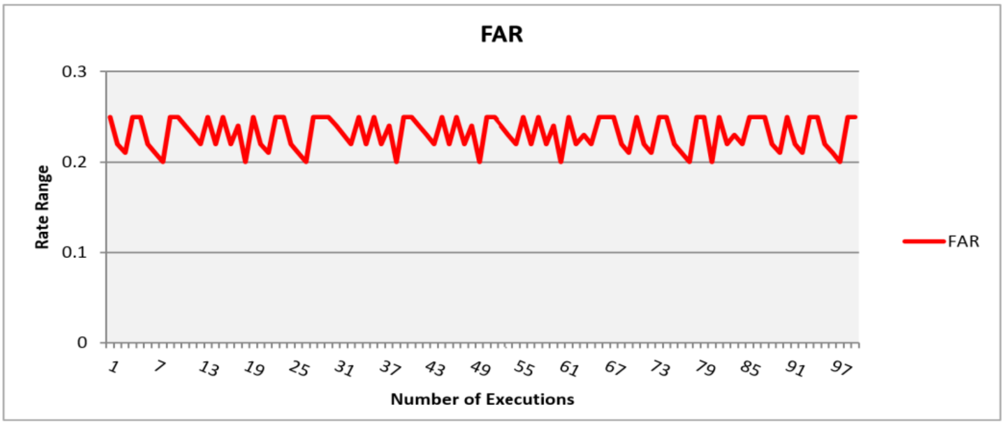


Fig. 19. FAR of the proposed system.

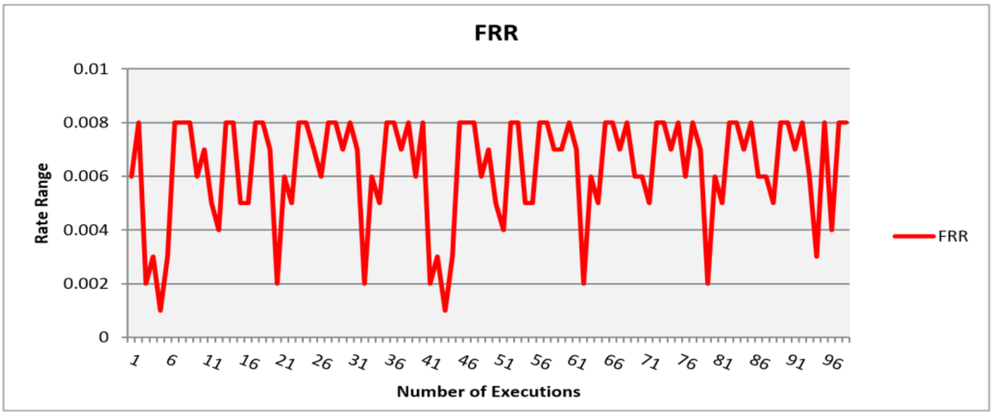


Fig. 20. FRR of the proposed system.

TABLE IV. FAR AND FRR OF THE PROPOSED SYSTEM AGAINST OTHER SYSTEMS

Healthcare system	**FAR**	**FRR**
[24] 2015	5.1%	0.1%
[25] 2018	5.84%	1.68%
Proposed system	0.25%	0.008%

- BCT transactions encryption and decryption performance: We perform execution time tests of BCT transactions encryption and decryption to test its acceptability as an encryption algorithm, as shown in Figure 21. We observed that the encryption and decryption operations of the ChaCha20 algorithm take execution times close to 0.0001 and 0.0008, respectively, which is very suitable for health transactions in PHRs. Furthermore, Table V provides a comparison between different encryption algorithms and the proposed algorithm, as well as some parameters used with these algorithms.

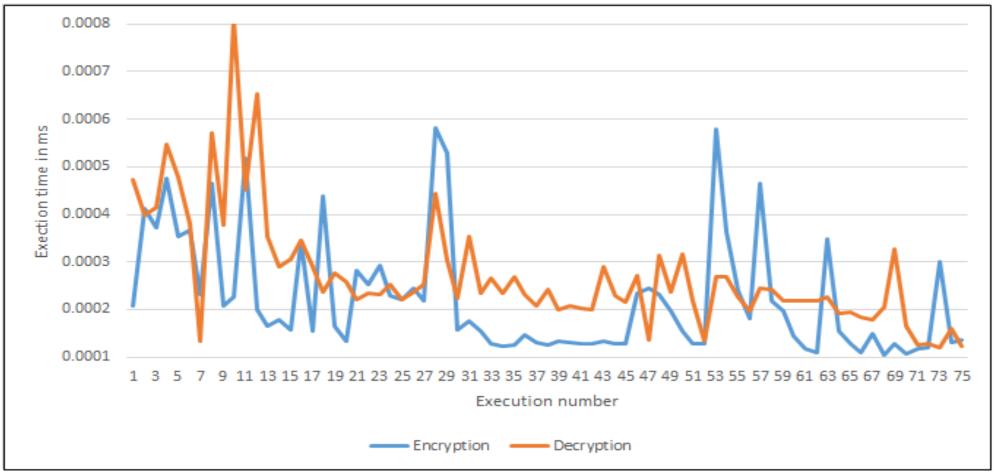


Fig. 21. ChaCha20 encryption and decryption for BCT transactions.

TABLE V. EVALUATION OF ENCRYPTION ALGORITHM PERFORMANCE ACROSS HEALTH SYSTEMS

System	Used encryption	Key length	App. type	Class of encryption	Type of algorithm	Execution time in ms	Requests No.	Bits No.	Supporting technology
[38]	AES	256	EHR	Standard	Symmetric	190	6	1000	GCM
[39]	ABSE	256	EMR	Standard	Asymmetric	-	7	2880	BCT
[40]	HABE	256	EMR	Standard	Symmetric	1.45	4	-	BCT
[41]	Blowfsh	256	EHR	Standard	Symmetric	2.012	4	1000	HCAC
[42]	AES/RSA	256	EHR	Standard	Asymmetric	24/5487	-	5000	XAMPP
Proposed	ChaCha20	256	PHR	Lightweight	Symmetric	0.0001-0.0008	2T	580	580 BCT

6. CONCLUSION

Comparing this amazing development, with the need to rely on a health system that those in charge of the health process can access in seconds and that is updated either through sensors placed in contact with the patient, is urgent and necessary in a world where the majority of daily routines are becoming increasingly automated. Since dealing with cancer patients is regarded as a crucial subject since we deal with their lives, we have proposed a security system to address their data, specifically to deal with cancer patients of all kinds. Compared with earlier studies, we proposed an integrated system that is thought to have the highest performance and secrecy in terms of both the high security offered by the system and the time required to retrieve, update data, or execution time for the system to finish the task. By fulfilling the following contributions, we conclude that digital health systems can rely on the proposed system, which operates on the idea of layers that are thought of as distinct from one another, to fulfill the necessary functions:

- Depending on the DS principle offers excellent security by separating patients into distinct groups based on the disease's characteristics. This technology offers a method of differentiating the features of the disease by comparing the parameters contained in it to produce a diagnosis, even though it offers excellent security because hacking one component does not impact the remaining components. It accurately determines the type of cancer, much like a doctor would.
- Since the data will not be changed or accessed until the smart contract's conditions—which are established by the NER—are satisfied, the NER algorithm and smart contracts function in tandem to complement one another. Storing and maintaining data without alteration are accomplished by using blockchain technology and ChaCha20 as a security repository.

- A high-performance compression method, such as SA, is used to lower the system resources, such as memory, that the proposed system uses.

For future trends, we plan to adopt postquantum signatures such as SPHINCS+ to support BCT. Also, we intend to expand our system analysis to repel quantum attacks. Finally, we intend to integrate zero-knowledge proofs with BCT to improve patient privacy in PHRs without revealing identities.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

There is no funding.

Acknowledgement

We would like to acknowledge the outstanding efforts of the editor and reviewers in reviewing and evaluating our research.

References

[1] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, “The benefits and threats of blockchain technology in healthcare: A scoping review,” International Journal of Medical Informatics, vol. 142, p. 104246, 2020, https://doi.org/10.1016/j.ijmedinf.2020.104246.

[2] R. H. Razzaq, M. Al-Zubaidie, and R. G. Atiyah, “Intermediary decentralized computing and private blockchain mechanisms for privacy preservation in the internet of medical things,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 152–165, 2024. [Online]. Available: https://doi.org/10.58496/MJCS/2024/020.

[3] A. Samadhiya, A. Kumar, J. A. Garza-Reyes, S. Luthra, and F. del Olmo García, “Unlock the potential: Unveiling the untapped possibilities of blockchain technology in revolutionizing internet of medical things-based environments through systematic review and future research propositions,” Information Sciences, p. 120140, 2024, https://doi.org/10.1016/j.ins.2024.120140.

[4] R. Agrawal and K. P. Patil, “Blockchain technology for medical records security using fit viability approach,” in 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT). IEEE, 2024, pp. 805–810, https://doi.org/10.1109/InCACCT61598.2024.10551119.

[5] R. H. Razzaq and M. Al-Zubaidie, “Formulating an advanced security protocol for internet of medical things based on blockchain and fog computing technologies,” Iraqi Journal for Computer Science and Mathematics, vol. 5, no. 3, pp. 723–734, 2024. [Online]. Available: https://doi.org/10.30880/ijcsm.2024.05.03.046.

[6] M. Al-Zubaidie and R. A. Muhajjar, “Integrating trustworthy mechanisms to support data and information security in health sensors,” Procedia Computer Science, vol. 237, pp. 43–52, 2024. [Online]. Available: https://doi.org/10.1016/j.procs.2024.05.078.

[7] M. Al-Zubaidie and W. A. Jebbar, “Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment,” Applied Sciences, vol. 14, no. 14, p. 6361, 2024, https://doi.org/10.3390/app14146361.

[8] J. K. Oladele, A. A. Ojugo, C. C. Odiakaose, F. U. Emordi, R. A. Abere, B. Nwozor, P. O. Ejeh, and V. O. Geteloma, “Behedas: A blockchain electronic health data system for secure medical records exchange,” Journal of Computing Theories and Applications, vol. 1, no. 3, pp. 231–242, 2024, https://doi.org/10.62411/jcta.9509.

[9] D. H. Tahayur and M. Al-Zubaidie, “Enhancing electronic agriculture data security with a blockchain-based search method and e-signatures,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 1–21, 2024, https://doi.org/10.58496/MJCS/2024/012.

[10] H. Bodur and I. F. T. Al Yaseen, “An improved blockchain-based secure medical record sharing scheme,” Cluster Computing, pp. 1–20, 2024, https://doi.org/10.1007/s10586-024-04414-6.

[11] R. H. Razzaq and M. H. Al-Zubaidie, "Maintaining security of patient data by employing private blockchain and fog computing technologies based on internet of medical things," Informatica, vol. 48, no. 12, 2024, https://doi.org/10.31449/inf.v48i12.6047.

[12] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, "Healthrec-chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data," Computer Networks, vol. 241, p. 110223, 2024, https://doi.org/10.1016/j.comnet.2024.110223.

[13] H. Sahu, S. Choudhari, and S. Chakole, "The use of blockchain technology in public health: Lessons learned," Cureus, vol. 16, no. 6, 2024, https://doi.org/10.7759/cureus.63198.

[14] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications," Sensors, vol. 23, no. 15, p. 6762, 2023, https://doi.org/10.3390/s23156762.

[15] M. Kuliha and S. Verma, "Secure internet of medical things based electronic health records scheme in trust decentralized loop federated learning consensus blockchain," International Journal of Intelligent Networks, vol. 5, pp. 161–174, 2024, https://doi.org/10.1016/j.ijin.2024.03.001.

[16] G. Lax, R. Nardone, and A. Russo, "Enabling secure health information sharing among healthcare organizations by public blockchain," Multimedia Tools and Applications, pp. 1–17, 2024, https://doi.org/10.1007/s11042-024-18181-4.

[17] W. A. Jebbar and M. Al-Zubaidie, "Transaction-based blockchain systems security improvement employing micro-segmentation controlled by smart contracts and detection of saddle Goatfish," SN Computer Science, vol. 5, no. 7, pp. 1–23, 2024, https://doi.org/10.1007/s42979-024-03239-9.

[18] T. G. Tregi and M. Al-Zubaidie, "Enhancing traffic data security in smart cities using optimized quantum-based digital signatures and privacy-preserving techniques," Mesopotamian Journal of CyberSecurity, vol. 5, no. 1, pp. 256–272, 2025. [Online]. Available: https://doi.org/10.58496/MJCS/2025/017.

[19] Y. Y. Ghadi, T. Mazhar, T. Shahzad, M. Amir khan, A. Abd-Alrazaq, A. Ahmed, and H. Hamam, "The role of blockchain to secure internet of medical things," Scientific Reports, vol. 14, no. 1, p. 18422, 2024, https://doi.org/10.1038/s41598-024-68529-x.

[20] V. Paul, S. Pandhi, D. K. Mahato, A. Agarwal, and A. D. Tripathi, "Polyhydroxyalkanoates (PHAs) and its copolymer nanocarrier application in cancer treatment: An overview and challenges," International Journal of Biological Macromolecules, p. 134201, 2024.

[21] A. Rehman, H. Xing, L. Feng, M. Hussain, N. Gulzar, M. A. Khan, A. Hussain, and D. Saeed, "FedCSCD-GAN: A secure and collaborative framework for clinical cancer diagnosis via optimized federated learning and GAN," Biomedical Signal Processing and Control, vol. 89, p.105893, 2024.

[22] K. C. Rath, A. Khang, S. K. Rath, N. Satapathy, S. K. Satapathy, and S. Kar, "Artificial intelligence (AI)-enabled technology in medicine-advancing holistic healthcare monitoring and control systems," in Computer Vision and AI-Integrated IoT Technologies in the Medical Ecosystem. CRC Press, 2024, pp. 87–108.

[23] A. Akingbola, A. Adegbesan, O. Ojo, J. U. Otumara, and U. H. Alao, "Artificial intelligence and cancer care in Africa," Journal of Medicine, Surgery, and Public Health, vol. 3, p. 100132, 2024.

[24] M. N. Dar, M. U. Akram, A. Usman, and S. A. Khan, "ECG biometric identification for general population using multiresolution analysis of DWT based features," in 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). IEEE, 2015, pp. 5–10.

[25] H. J. Kim and J. S. Lim, "Study on a biometric authentication model based on ECG using a fuzzy neural network," in IOP conference series: Materials science and engineering, vol. 317, no. 1. IOP Publishing, 2018, p. 012030.

[26] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble, and R. A. Dziyauddin, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," Sustainability, vol. 15, no. 8, p. 6337, 2023, https://doi.org/10.3390/su15086337.

[27] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," Journal of medical systems, vol. 43, pp. 1–9, 2019, https://doi.org/10.1007/s10916-018-1121-4.

[28] N. Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," Complex & Intelligent Systems, vol. 8, no. 1, pp. 625–640, 2022, https://doi.org/10.1007/s40747-021-00549-w.

[29] A. Ibor, E. Edim, and A. Ojugo, "Secure health information system with blockchain technology," Journal of the Nigerian Society of Physical Sciences, pp. 992–992, 2023, https://doi.org/10.46481/jnsps.2023.992.

[30] L. Ismail, H. Materwala, and S. Zeadally, “Lightweight blockchain for healthcare,” IEEE access, vol. 7, pp. 149 935–149 951, 2019, https://doi.org/10.1109/ACCESS.2019.2947613.

[31] A. Ojugo and D. Otakore, “Improved early detection of gestational diabetes via intelligent classification models: A case of the niger delta region in Nigeria,” Journal of Computer Sciences and Applications, vol. 6, no. 2, pp. 82–90, 2018, https://doi.org/10.12691/jcsa-6-2-5.

[32] A. Rehman, S. Abbas, M. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, “A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique,” Computers in Biology and Medicine, vol. 150, p. 106019, 2022, https://doi.org/10.1016/j.compbiomed.2022.106019.

[33] A. H. Al-Tameemi, et al. "A Systematic review of metaverse cybersecurity: Frameworks, challenges, and strategic approaches in a quantum-driven era." Mesopotamian Journal of CyberSecurity 5.2 (2025): 770-803. [Online]. Available: https://doi.org/10.58496/MJCS/2025/045.

[34] F. Hazzaa, M. M. Hasan, A. Qashou, and S. Yousef, “A new lightweight cryptosystem for IoT in smart city environments,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 46–58, 2024. [Online]. Available: https://doi.org/10.58496/MJCS/2024/015.

[35] B. Rashidi, “High-performance hardware structure of ChaCha20 stream cipher based on sparse parallel prefix adder,” International Journal of Circuit Theory and Applications, vol. 53, no. 5, pp. 2947–2957, 2025. [Online]. Available: https://doi.org/10.1002/cta.4264.

[36] L. M. Martínez Guevara, P. J. Vidal, A. C. Olivera, and E. N. Millán, “Analysis and comparison of encryption and verification algorithms applied to a fog computing architecture,” Journal of Information and Telecommunication, vol. 9, no. 2, pp. 173–189, 2025. [Online]. Available: https://doi.org/10.1080/24751839.2024.2411884.

[37] N. K. Upadhyay, P. Sudhakar, and V. Kumar, “Efficient cryptographic configurations and lightweight communication protocols for secure smart home systems,” in 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI), vol. 3. IEEE, 2025, pp. 657–662. [Online]. Available: https://doi.org/10.1080/24751839.2024.2411884.

[38] K. S. K. Maathavan and S. Venkatraman, “A secure encrypted classified electronic healthcare data for public cloud environment.” Intelligent Automation & Soft Computing, vol. 32, no. 2, 2022. [Online]. Available: https://doi.org/10.32604/iasc.2022.022276.

[39] G. Liu, H. Xie, W. Wang, and H. Huang, “A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption,” Journal of cloud computing, vol. 13, no. 1, p. 44, 2024. [Online]. Available: https://doi.org/10.1186/s13677-024-00608-w.

[40] E. Zaghloul, T. Li, and J. Ren, “d-EMR: Secure and distributed electronic medical record management,” High-Confidence Computing, vol. 3, no. 1, p. 100101, 2023. [Online]. Available: https://doi.org/10.1016/j.hcc.2022.100101.

[41] P. Chinnasamy and P. Deepalakshmi, “HCAC-EHR: Hybrid cryptographic access control for secure EHR retrieval in healthcare cloud,” Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 2, pp. 1001–1019, 2022. [Online]. Available: https://doi.org/10.1007/s12652-021-02942-2.

[42] S. A. Ajagbe, H. Florez, and J. B. Awotunde, “AESRSA: A new cryptography key for electronic health record security,” in International Conference on Applied Informatics. Springer, 2022, pp. 237–251. [Online]. Available: https://doi.org/10.1007/978-3-031-19647-8_17.