RESEARCH PAPER

Dynamic Key-Driven Secure Framework for Patient-Centric Cloud Health Record Sharing With Enhanced Attack Resilience

[1*]Naveen John J and [2]I. Shatheesh Sam

[1]Department of Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India*
[2]Associate Professor in the Department of PG Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India
***Corresponding Author:** naveenjohnj41@gmail.com*

Received: 24th April, 2026; Revised: 20th May 2026; Accepted: 30th June, 2026; Available Online: 10th July, 2026

ABSTRACT
The vast growth of digital health services and the rising number of cyber attacks targeting sensitive medical information have made the management and security of patient health records (PHRs) in cloud settings a pressing issue. Nearly a quarter of all reported data breaches in the healthcare industry involved data from this sector and the average cost of a breach was over USD 10 million, underscoring the critical need for effective, scalable, and privacy-preserving solutions. In traditional systems, cryptographic methods like RSA, ECC, and Attribute-Based Encryption (ABE) can be inefficient for large numbers of attributes and users, as well as vulnerable to brute force and unauthorized access attacks in dynamic cloud environments. To tackle these challenges, this study introduces a security enhanced patient-centric cloud (SPCC) system which not only utilizes an adaptive key generation method using a dynamic RSA (DRSA) algorithm that utilizes a hybrid black widow optimization and sine cosine (HBSC) algorithm, but also employs attribute-based encryption to implement fine-grained access control over patient sensitive medical records. The proposed framework is validated with multiple large-scale healthcare datasets, such as MIMIC-IV, eICU collaborative research database, PhysioNet challenge datasets and HiRID, which includes various ICU and physiological data. The DRSA-HBSC framework can reach the attack resistance of up to 14.29% better than RSA, ECC, and ABE while its security score is up to 9.62% higher, and encryption/decryption time is reduced by 49.18 % and 48.96 % respectively. There is 12% reduction in memory usage and communication delays. Secure and efficient sharing of PHR is assured by good robustness as reflected by a Brier score of 0.041 and Cohen's Kappa of 0.921.

Keywords: patient health records, cloud security, data privacy, access control, healthcare data management, scalable encryption

How to cite this article: John NJ, Sam IS, Dynamic Key-Driven Secure Framework for Patient-Centric Cloud Health Record Sharing With Enhanced Attack Resilience. Int J Drug Deliv Technol. 2026;16(77s): 1713-1734; DOI: 10.25258/ijddt.16.77s.197
Source of support: Nil.
Conflict of interest: None

1. INTRODUCTION

Digital healthcare systems are rapidly evolving and the cloud is increasingly being adopted to manage and share medical data, changing the landscape of healthcare information management and sharing. Personal Health Records (PHRs) are patient-centric digital archives enabling individuals to manage, control and access their lifelong health data, which comes from various sources such as hospitals, clinicians, pharmacies and patient-generated devices [1, 2]. Patient-generated health data (PGHD) has grown with the advent of wearable devices and mobile health apps, allowing for the continuous collection of data and the delivery of personalized healthcare [3, 4]. The PHRs are different from the conventional electronic health records (EHRs) because they give patients more autonomy over their medical data and allow interoperability between health care providers [5, 6]. Because of its scalability, cost effectiveness, and availability, cloud computing is a key enabling technology for storing and sharing PHRs [7, 8]. But the security and privacy concerns with third-party cloud servers are also quite a challenge, such as unauthorized access, insider threat, data leakage, and cyber attacks [9, 10]. Healthcare was reported to be one of the most common sectors targeted, with a large portion of data breaches occurring in the healthcare sector, with serious financial and privacy implications [11]. PHRs are sent via open networks, and are susceptible to interception attacks, key compromise and unauthorized disclosure of information [12]. So far, numerous cryptographic ideas have been studied in order to reduce these risks. Routine symmetric encryption methods are computationally efficient but they have complex key distribution and management problems in a large-scale application [13]. Security in the distribution of keys is enhanced by asymmetric encryption methods like RSA and ECC, but their computational requirements are

**Author for Correspondence: naveenjohnj41@gmail.com*

more complex for the use of large medical datasets [14]. ABE is a well-known method that has been widely explored in the context of fine-grained access control in the cloud by allowing access to data based on user attributes like role, department or privileges [15, 16]. The searchable encryption techniques have been proposed to ensure secure querying over encrypted medical data without disclosing any sensitive information [17]. Hybrid security models, which integrate various security mechanisms like encryption, authentication, and access control, have also been explored to improve data security in healthcare cloud environments [18].

Current solutions still have some issues with scalability, computational efficiency, dynamic key management, and protection against new cyber threats. Moreover, mHealth and IoT healthcare system comes with further constraints of limited processing capability, energy efficiency, and interoperability challenges across the heterogeneous platforms [19, 20]. The challenges these restrictions present are clear, underlining the need for more flexible and secure structures that can enable the effective and privacy-conscious handling of patient's health information in the cloud. A solution to overcomes the challenges of mobile health systems, an enhanced, patient-centric cloud (SPCC) framework using Dynamic RSA (DRSA) key generation along with hybrid black widow optimization and sine cosine (HBSC) algorithm. The proposed SPCC framework has improved the resisting ability of the encrypting key against the attack of brute force, reduced the needed computation resources for encrypting/decrypting the data, and applied the attribute-based encryption (ABE) technology to achieve fine-grained access to secured patient health records (PHRs). By establishing optimized RSA encryption keys with HBSC, the SPCC framework provides security, performance, and scalable management of PHRs in the cloud, helping to address the limits of existing cloud PHR models and support patient-centric health care. The key contribution of the proposed framework is given as follows.

- This study presents a SPCC framework specifically designed to ensure secure, efficient, and scalable management of PHRs in cloud environments.
- The framework utilizes the dynamic key generation mechanism that enhances cryptographic strength and reduces computational overhead, thereby improving resistance against brute-force and related security attacks.
- It incorporates attribute-based encryption (ABE) to enable fine-grained, patient-centric access control, ensuring that only authorized users with appropriate credentials can access sensitive medical data.
- The effectiveness of the proposed framework is validated using multiple large-scale healthcare datasets, including MIMIC-IV, eICU Collaborative Research Database, PhysioNet Challenge datasets, and HiRID.

The paper is organized as follows: Section 2 reviews related work, Section 3 presents the proposed SPCC framework and datasets, Section 4 discusses results and analysis, and Section 5 concludes the study.

2. RELATED WORK

An access control system for healthcare has been introduced that combines role-based access control, attribute-based policies, and real-time anomaly detection based on healthcare data to ensure user authentication and security of sensitive medical details [21]. Dynamic decryption token generation further reinforces secure data retrieval, although the static policy definition and rule configuration reduces the ability to adapt in very dynamic cloud environments, impacting scalability in large-scale deployments. An EHH multiple tier encrypted architecture is developed through natural language processing – based data structuring, secure key management, and cloud-based storage mechanism for ensuring confidentiality and controlled access to sensitive patient records [22]. While this enhances structured data management and ensures better privacy protection, it also adds to the computational burden, as the data needs to be preprocessed, and heavily depends on centralized cloud systems which could affect system performance in latency-critical healthcare applications. Reinforcement learning-based key generation for biometric authentication and symmetric encryption mechanisms have also been proposed as advanced authentication systems in addition to decision tree-based anomaly detection for detection of abnormal access behavior [23]. These multiple-layered security architectures enhance adaptive security and intrusion detection, however they add to the complexity of their operations and they are not ideal for the resource-limited healthcare applications. In healthcare systems, blockchain technology can be used to enhance electronic health record (EHR) security, facilitate patient data tracking, and implement role-based access control and QR code authentication during data sharing [24]. Decentralized patient-centric health record systems (DRPHS) using distributed ledger technologies (DLT) and NFTs for health record ownership give patients more control and transparency over their health records and enable access to healthcare providers with permission [25]. However, these systems have a number of drawbacks, including scalability, high transaction fees, and compatibility with current healthcare systems, which limit their use in actual healthcare environments.

To enable secure transmission and storage of patient health records in cloud environments, hybrid cryptographic models using digital signatures, symmetric cryptographic schemes and optimization-based key generation methods have been proposed [26]. These methods improve the robustness and the efficiency of the encryption; however, hybrid optimizations will make the algorithm more complex, thereby resulting in greater running time for large data sets. More advances have been made to enhance

key generation and improve encryption performance in EHR systems, incorporating metaheuristic optimization techniques, hashing algorithms and elliptic curve cryptography [27]. These frameworks provide improved security robustness and alleviate some computational limitations, but their adaptability in highly dynamic cloud settings is not robust and they may not prove effective in dealing with changing attack patterns in cyber warfare. High-dimensional quantum key distribution (QKD) methods are applied in quantum-inspired secure communication protocols for IOT (IOT) and eHRs (EHRs), where the security gateways are located at the edges of the network to ensure security in the transmission of the key [28]. These models may offer robust theoretical security assurances and greater error resilience, but they are not readily practical, constrained by hardware limitations, implementation complexity, and scalability to real-world applications. Distributed storage and blockchain-based healthcare security models combine interplanetary file systems, asymmetric encryption and reputation-based consensus to improve data integrity, its sharing and storage efficiency [29]. For secure medical record management, lightweight authentication and encryption frameworks, based on smart card-based verification, hash-based security mechanisms, and metaheuristic optimization techniques, have been proposed [30]. While these models enhance the security of authentication and encryption, they introduce additional layers of security and may result in a higher computational cost and lower efficiency in large-scale cloud systems.

Problem definition: Although much has been undertaken to secure cloud healthcare systems, there are some problems that still need to be addressed. Various methods (Table 1) have been proposed to ensure privacy, but are based on static policies and are not scalable for the dynamic cloud computing environment [21]. Multi-level encryption and hybrid encryption schemes increase the level of security achieved, but also add significant computational cost and latency, making them unsuitable for processing large-scale healthcare data in a timely and efficient manner [22, 23, 26, 27]. Despite offering transparency and decentralized control, blockchain and NFT-based patient-centric models have weaknesses, such as transaction delays, costs, and issues with interoperability [24, 25, 29]. Theoretically, quantum key distribution and key generation based on optimization improve security, but it is difficult to deploy practically due to hardware limitations, algorithmic complexity, and lack of adaptability to real-time cloud operations [28, 30]. The restrictions underscore the necessity of a lightweight, scalable, and dynamic patient-centric cloud system that enables secure, efficient, and fine-grained management of EHRs in real-world healthcare scenarios.

Table 1 Comparative analysis of existing patient-centric cloud security frameworks and research gaps

Ref	Motivation	Methodology	Dataset used	Key findings	Research gap	How SPCC addresses gap
[21]	Secure access and monitoring of PHRs in cloud	RBAC + Attribute-based policies + Anomaly detection	MIMIC-III	Unauthorized access reduced by 75%	Static policies, limited scalability	Dynamic key generation + ABE, scalable access control
[22]	Protect EHH privacy in cloud storage	Multi-tier encryption + NLP + Key management	AWS Cloud, simulated EHH	Encryption latency ~2.5s per record	High computational overhead, centralized dependency	Lightweight dynamic encryption reduces computation
[23]	Adaptive authentication with anomaly detection	Biometric + Camellia + Q-learning + Decision tree	Simulated health data	Key entropy 128-bit, unauthorized attempts detected 90%	Complex layered mechanism, high computation	Optimized key generation reduces overhead
[24]	Secure blockchain-based EHR management	Blockchain + RBAC + QR-code access	Hospital EHR logs	Data integrity 99%, access delay ~1.8s	Blockchain latency, energy-intensive	Efficient cryptography reduces latency, retains integrity
[25]	Decentralized patient control over PHR	NFT + Hyperledger Fabric	Simulated patient records	Transaction success rate 95%	High transaction cost, limited interoperability	Optimized key + ABE ensures low-overhead access control
[26]	Secure PHR sharing	Signcryption + AES + Optimized key	MIMIC-III	Encryption time 1.2s, accuracy 98%	High algorithmic complexity	SPCC uses efficient dynamic key

						generation
[27]	Improve EHR key generation and encryption	CS + SHA-256 + ECC	Simulated EHR	Key generation time 0.8s, encryption success 97%	Limited adaptability, evolving attack risk	Dynamic key + optimization handles large-scale dynamic data
[28]	Secure IoMT & EHR transmission	HD-QKD + Edge security gateways	IoMT Testbed	Transmission error <2%, security level 95%	Hardware constraints, complex deployment	Lightweight cloud-based key system, no hardware dependency
[29]	Privacy-preserving archival sharing	Blockchain + IPFS + Multi-prime encryption	Simulated medical archives	Throughput 120 transactions/s, delay 2.1s	High computational cost, latency	Efficient cloud encryption and fast access reduces delay
[30]	Strengthen authentication & PHR protection	Smart card + Random-hash + SSO + Feistel	Hospital PHR	Accuracy 96%, encryption strength 92%	High computation overhead	Dynamic key, ABE algorithm reduces computational load

3. MATERIALS AND METHODS

The views of the proposed conceptual diagram of secure patient-centric cloud health information sharing are shown in Figure. 1. The framework starts with healthcare data acquisition, in which data is collected from various sources, such as MIMIC-IV, eICU Collaborative Research Database, PhysioNet Challenge datasets, HiRID, hospital EHR/PHR systems, and wearable devices, and serves as a consolidated raw healthcare data repository [31, 32, 33]. Data preprocessing and attribute extraction comes next, where missing values in the data are filled and noise is removed, along with normalizing the data and identifying attributes of the patient, doctor role, department, disease type, access privileges, treatment category, location and time. This means that the healthcare dataset is cleaned, and an attribute set (AS) is created and structured, making the data suitable for secure processing. The HBSC optimization engine is then applied as a key parameter tuning technique which combines Hybrid Black Widow Optimization (HBWO) and Sine Cosine Algorithm (SCA). This process determines optimum parameters of RSA key, which have maximum key strength, security level and minimum memory consumption, computation and encryption/decryption time and generates optimum set of RSA parameters (p, q, e, d, n). A periodic key-refresh mechanism is used to ensure high cryptographic security and these parameters are used in the Dynamic RSA (DRSA) key generation. For fine-grained access policies, such as "(Doctor AND Cardiology) OR (Admin AND Hospital_A) OR (Nurse AND ICU)", where only specific users should be able to access sensitive healthcare information, Attribute-Based Encryption (ABE) is applied to ensure that only those users who possess the necessary attributes (e.g. Doctor, Cardiology) or (Admin, Hospital_A) or (Nurse, ICU) are granted access. The result is PHRs encrypted according to ABE, access control policies, and ciphertext. The Security-Enhanced Patient-Centric Cloud (SPCC) is a secure, scalable, and trusted cloud-based environment that offers secure data storage, management, indexing, metadata handling, access control, data integrity, and availability, ensuring robust and reliable cloud data management for healthcare organizations. Authorized user requests are checked against access policies and attributes; if they are authorized, DRSA and ABE decryption are performed on the patient health records, and access granted, otherwise access is denied for unauthorized users.

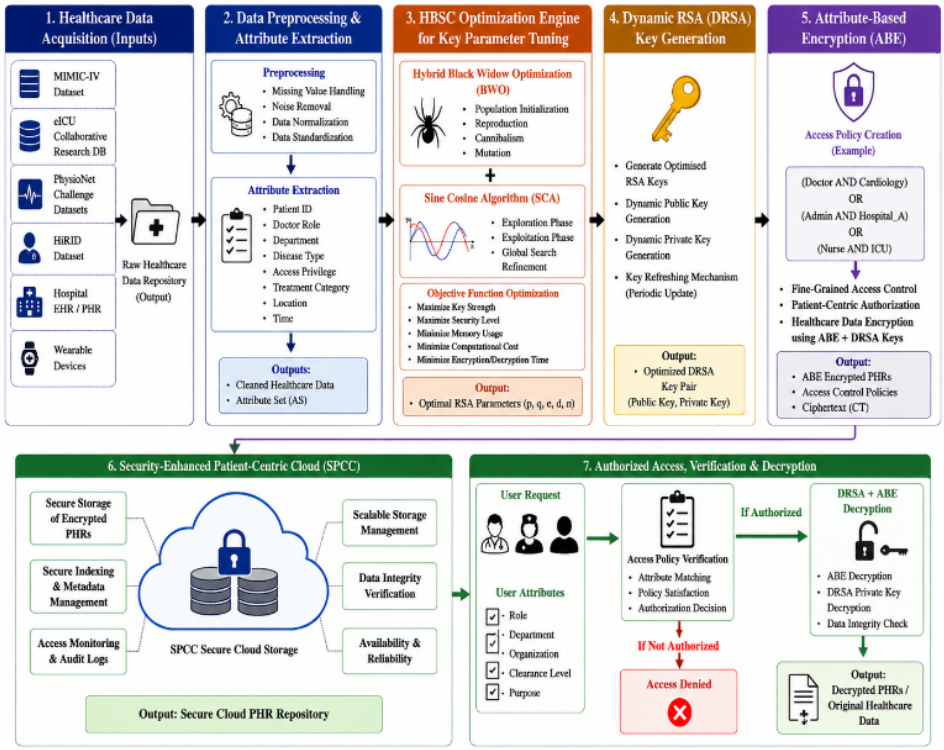

Figure. 1 Conceptual structure of proposed SPCC framework for secure, efficient, and scalable management of PHRs in cloud environments

3.1 Data preparation

Four well known healthcare datasets, MIMIC-IV, eICU Collaborative Research Database (eICU-CRD), PhysioNet Challenge datasets, and HiRID were used to evaluate the proposed SPCC framework. These datasets were chosen as a result of their rich clinical content, patient volume, high-resolution physiological data, and the diversity of healthcare data that they represent, allowing for the evaluation of cloud-based health information sharing systems in terms of security, scalability, and efficiency. The datasets all include structured and unstructured clinical records, laboratory measurements, diagnostic information, vital signs, and time-series observations from intensive care and physiological monitoring settings. The MIMIC-IV database includes information from 382,278 patients and 73,181 patient stays in an ICU between 2008 and 2019, with over 200 clinical variables and more than 100 laboratory measurements. The eICU-CRD data set consists of 139,367 patients and 200,859 ICU admissions from over 200 hospitals, providing a large-scale, multihospital clinical setting to test secure healthcare data management. The PhysioNet Challenge datasets provide over 40,000 physiological records at very high temporal resolution, so that the framework can be evaluated in continuous monitoring setting. The HiRID is a dataset of 33,904 ICU admissions and over 700 clinical variables at minute-level resolution that enable detailed study of security mechanisms in high frequency healthcare data streams. The datasets vary in size, in their spatial and temporal time frame, in the degree of clinical complexity and in the extent of healthcare coverage, thus offering a full-scale reference for testing the soundness of the proposed framework. MIMIC-IV and HiRID provide abundant clinical and laboratory data and eICU-CRD provides large multicenter data for scalability assessment. The PhysioNet datasets focus on physiological time series monitoring, however, with very high resolution measurements. These datasets can be used to evaluate the proposed SPCC framework in various healthcare applications such as critical care management, physiological monitoring, real-time patient monitoring, and medical data sharing over large-scale cloud networks. All the datasets were preprocessed before being used for security processing, which involved missing data, normalization, data extraction, and record standardization to facilitate handling of shared data from heterogeneous sources. The below table 2 shows the Statistical description of healthcare datasets used for evaluation.

Table 2 Statistical description of healthcare datasets used for evaluation

Attribute	MIMIC-IV	eICU-CRD	PhysioNet	HiRID
Year released	2020	2018	Multiple	2021
Source institution	Beth Israel Deaconess Medical Center	Multi-center US Hospitals	PhysioNet Research Community	Bern University Hospital
Patients / admissions	382,278 Patients	139,367 Patients	>40,000 Records	33,904 Patients

ICU stays / admissions	73,181 ICU Stays	200,859 ICU Admissions	N/A	33,904 ICU Admissions
Number of Hospitals	1	>200	Multiple Sources	1
Clinical variables	>200	>150	>50	>700
Laboratory measurements	>100	>80	Varies	>100
Vital sign parameters	>20	>15	>30	>25
Time-series resolution	High Resolution	High Resolution	Very High Resolution	Minute-Level Resolution
Sampling frequency	Event-Based	Event-Based	Second-to-Minute Level	Minute-Level
Demographic information	Available	Available	Limited	Available
Diagnosis information	ICD Codes	ICD Codes	Challenge Specific	ICD Codes
Procedure information	Available	Available	Limited	Available
Clinical notes	Available	Limited	Not Available	Limited
Structured data	Yes	Yes	Partial	Yes
Unstructured data	Yes	Limited	No	Limited
Data period	2008–2019	2014–2015	Multiple Years	2008–2016
Data type	Structured & Unstructured	Structured	Physiological Time-Series	Time-Series & Structured
Data volume	~7.5 GB	~88 GB	~5–20 GB	~9 GB
Data accessibility	Open research access	Open research access	Open research access	Open research access
Healthcare domain	Critical Care	Critical Care	Physiological Monitoring	Critical Care
Security evaluation suitability	High	High	Moderate	High
Scalability evaluation suitability	High	Very High	Moderate	High
Real-time monitoring capability	Moderate	Moderate	Very High	High

3.2 HBSC-based dynamic key optimization

The PHRs are highly vulnerable in a cloud-based health care system if the encryption keys are not strong enough and have low randomness. Common key generation techniques include static keys and pseudo-random keys, both of which can be susceptible to brute force attacks and aren't necessarily well suited for the dynamic nature of cloud computing where data can be large in scale and highly heterogeneous. To solve these drawbacks, the suggested framework makes use of a hybrid black widow optimization and sine cosine (HBSC) algorithm to dynamically generate optimized RSA keys that improves security level and computational efficiency. In fact, the HBSC algorithm is a metaheuristic optimization algorithm that provides a perfect balance between global search and local search; the black widow optimization combines the global search capabilities while the sine cosine algorithm adds the exploratory strength, resulting in an algorithm that has proven to yield highly unpredictable encryption keys that are resistant to attacks. Key generation factors considered are patient specific, numerical representation of medical attributes like age, vital signs, lab parameters, key space, allowed key space, and cryptographic constraints. The HBSC-based algorithm achieves dynamic adaptation in key generation, generates keys based on patient and system-specific parameters, avoids local minima, requires less computation because keys are optimized to represent fewer bits, and is more secure due to increased key entropy, compared with the conventional key generation method or any standalone metaheuristic algorithm. The proposed SPCC framework overcomes the drawbacks of the current static or computationally demanding approach to key generation by incorporating HBSC-based dynamic key optimization to enable secure, efficient, and scalable management of PHRs in cloud environments. HBSC algorithm starts with a set as the starting private key that is generated randomly. Key values are used to randomize the position of black widow. Each problem's potential solution $\left(R_{private}^{key}\right)$ is seen by the black widow spider. The values of the problem variables are displayed by each black widow spider. When solving benchmark functions, the structure should be considered an array. The dimensional optimization problem is denoted by the variable M_v and

the matrix population by the variable M_p . The problem system is evaluated by a widow (d), which is an array of M_v, describes as follows.

$$d = \left\lfloor y_1, y_2, y_3, ..., y_{M_v} \right\rfloor \quad (1)$$

Each variable's floating-point number is $\left(y_1, y_2, y_3, ..., y_{M_v}\right)$, and the widow's fitness denotes as S.

$$S = S\left(y_1, y_2, y_3, ..., y_{M_v}\right) \quad (2)$$

To begin the optimization problem, the spider's initial population (P) with the candidate matrix size ($M_p \times M_v$) is created. The pairs are distinct in the BWO algorithm, and they start to mate to create a new generation by mating with each other individually. At last, the spider babies are maturing and becoming very strong. As a result, it is generated using a long window array and a random generation method. The best individuals are gathered and added to the newly created population. The process of procreate is stated as follows, based on the offspring operation.

$$\begin{cases} V^1 = \alpha w^1 + (1-\alpha) V^2 \\ V^2 = \alpha w^2 + (1-\alpha) V^1 \end{cases} \quad (3)$$

There are three types of cannibalism (i) the position of the black widow is randomized using the key values (i.e., sexual cannibalism) (ii) stronger siblings devour weaker siblings (i.e., sibling cannibalism) and (iii) Sometimes the young spiders consume the mother spider. The fitness values are used to determine which spider lings are strong and which are weak. In this stage, the number of people in the population of silent pop is chosen at random. Every solution is chosen at random after swapping two items in the array. The mute pop is computed using the mutation rate. To expand the complexity, avoid premature convergence, and convergence speed needs to be accelerated with the SCA algorithm. Here, termination is done based on the results obtained from the fitness value, and until it reaches the overall iteration. The SCA helps to enhance the BWO's performance based on its optimization strategy as follows.

$$p_{ij}(t+1) = \begin{cases} p_{ij}(t) + r_1 \sin(r_2) \times \| R_3 \operatorname{Pr} ob_j - p_{ij}(t) \| & if \;\; r_4 < 0.5 \\ p_{ij}(t) + r_1 \cos(r_2) \times \| R_3 \operatorname{Pr} ob_j - p_{ij}(t) \| & if \;\; r_4 \geq 0.5 \end{cases} \quad (4)$$

The aforementioned equation helps to update the performance of BWO, the optimized key can be more effectively selected than the traditional BWO. Select the best key as the best key for the RSA-based encryption and decryption operations from all of the keys. The sender's optimal private key is denoted by $O_{sprivate}^{key}$, the optimized private key of the receiver is denoted by $O_{rprivate}^{key}$ in this example. As describes in Algorithm 1, the outcomes of this process include highly secure, patient-specific RSA keys, reduced encryption and decryption times, lower memory consumption, and increased robustness against unauthorized access.

Algorithm 1 Pseudo-code of the HBSC-based dynamic key optimization process

Inputs	Patient identifiers, clinical attributes, key length, key space, cryptographic constraints, population size, max iterations, mutation rate
Outputs	Optimized sender private key, optimized receiver private key
1	Initialize population of candidate keys randomly
2	Evaluate fitness of each candidate based on security and entropy
3	Set iteration = 0
4	While iteration < max iterations do
5	For each candidate in population do
6	Pair candidate with another randomly selected candidate
7	Generate offspring from mating
8	End For
9	For each offspring do
10	If random < sexual_cannibalism_rate then
11	Randomize positions of candidate

12	End If
13	If candidate is weaker than sibling then
14	Replace weaker candidate with stronger sibling
15	End If
16	If candidate is weaker than parent then
17	Replace parent with offspring
18	End If
19	End For
20	Apply Sine Cosine Algorithm to update candidate positions
21	For each candidate do
22	If random < mutation rate then
23	Apply small random change to candidate
24	End If
25	End For
26	Evaluate fitness of updated population
27	Select candidate with highest fitness as current best key
28	If convergence criteria met then
29	Break
30	End If
31	iteration = iteration + 1
32	End While
33	Return best candidate as optimized sender private key, best candidate as optimized receiver private key

3.3 Dynamic RSA (DRSA) Key Generation

The proposed framework uses dynamic RSA (DRSA) as the cryptographic mechanism to protect Patient Health Records (PHRs) in the sharing of healthcare information in the cloud. The DRSA module performs three key steps – key generation, encryption, and decryption – and incorporates a message authentication code (MAC) mechanism to ensure data integrity. After the pre-processing, the healthcare records are sent to the key generation center (KGC) that acts as a trusted authority to generate cryptographic parameters. In the key generation process, two large prime numbers (p) and (q) are chosen to calculate the RSA modulus (n=pq), and Euler's totient function (phi(n)=(p-1)(q-1)). Then, a public key (e, n) and a private key (d, n) are generated and a public exponent e is generated with a private exponent d. The proposed approach uses the hybrid black widow optimization and sine cosine (HBSC) algorithm, which differs significantly from conventional RSA, to optimize the selection of these parameters according to the security strength, computational complexity, memory demands and attacks resistance. The optimized parameters are then securely distributed to the patient (PA), the receiver (Re) and the cloud server (CS). The key generation is done, and then the encryption phase is done. The generated RSA public-key is dynamically sent to the patient, who then encrypts the healthcare data prior to uploading to the cloud environment. Prior to encryption, a secret key s and message m are processed using MAC based on the SHA-256 hash function to ensure message authenticity and integrity. The patient's health data (including the authentication codes) is then uploaded and stored in the security-enhanced patient-centric cloud (SPCC) system. The cloud computer is used for encrypted data and ensuring the availability of data, and without access to the plaintext data. If a legitimate health care provider or authorized user requests access to patient information, the decryption phase begins. Once authenticated, the receiver pulls down the encrypted records from the cloud, but before the records are decrypted, the receiver checks the MAC value against the shared secret key. Matching MAC values are signatures provided to ensure that the data transmitted has not been modified. The recipient uses his/her own RSA private key to decrypt the ciphertext and retrieve the original patient information. RSA plays a security model for encrypting the patient data, i.e., represented as PA. The PA stores data more securely using the DRSA algorithm, where the keys of receivers are public key PK_{ur} and the key of senders as private key $PK_{s,}$explicitly with the key s. DRSA, being a public-key ciphering applies a secret public key $PK_{ur}$to encrypt the data. Use private key $PK_{s}$to work on the decryption of the RSA-encrypted data at the receiver.

$$C = \left\{E_{RSA}, P_{Data}, \hat{P}_{Data}, PK_{ur}, PK_{s}\right\} \quad (5)$$

$$\hat{T}_{even} = \left\{E_{RSA}\left(T_{even}, PKur\right)\right\} \quad (6)$$

The Re looks for information by sending it to the cloud. Using PK_r, the receiver's private key, and PK_{ur}, the sender's public key. Because of its large store capacity and powerful computer, the CS can oversee and maintain thePA's data. In essence, it's a partially trustworthy creature. Upon successful access, the receiver provides the corresponding data. The DRSA is dealing with the 64-bit RSA for improving the computation efficiency. The user uses the RSA framework to develop the secret key during the verification process, as well as to decrypt data. The delivered data are in the form of a block cipher where an RSA-based approach is processed. In the patient-centric health care system, the DRSA algorithm has three processes: encryption, decryption, and key generation. The secret key (s) and the message (m) are altered one-way using MAC (s). For the MAC to be prepared, both sender and recipient must know a mutual symmetric (secret) key. MAC includes cryptography processing.

$$HMAC(text,s) = H\left[S_{out} \parallel H\left(S_{in} \parallel text\right)\right] \quad (7)$$

where H is the SHA256 algorithm's hash function, S_{out} and S_{in} are the two keys created from s, text is the text hashed with the key s, and || is concatenation. The following are the methods for constructing the secret key

$$S_{out} = s \oplus Opad \quad (8)$$

$$S_{in} = s \oplus Ipad \quad (9)$$

where $\oplus$stands forthe XOR operation. Before encrypting data, the key generation processes are carried out. Public service and the data user also facilitate RSA key generation. Encryption is the action of transforming extract text data from original or primary plain text data.

$$\alpha(C) = \alpha'(C) \quad (10)$$

Improvement is required for the entire day's secure transmission. The dynamic key refreshing capability of DRSA continuously updates cryptographic parameters, making it significantly more difficult for attackers to compromise keys through cryptanalytic attacks. Algorithm 2 describes the DRSA-based secure healthcare data transmission and access control process

Assume sender A wishes to communicate with Recipient B. No one else knows about the symmetric (secret) key S for A and B. A creates the MAC by using key S to message (m).

- The original message (m) and the MAC H 1 are then transmitted to B by A.
- B used s to calculate its own MAC H 2 over when it received the message.
- If H1 and H2 compare B, it's safe to assume that the message m hasn't changed during transits.
- If H 1H 2, however, B declines the message because during transit, the message was changed.

Hash MACs are hash transformations that are parameterized with secret key which is design of $MAC(m,s)$.

s: Consider s, which is x -bytes long and has the values o_{pad} and i_{pad}, and evolves x repetitions of the byte 01011100 and 00110110. Then

Decryption is the reversible encryption method. Decryption refers to the manner of converting primary simple text data into peppy text data. However, there is a chance of a brutal attack in which the key is broken, and the security key created as follows:

Algorithm 2 DRSA-based secure healthcare data transmission and access control process

Inputs	Preprocessed healthcare records, sender information, receiver information, optimized RSA parameters, secret key, authentication code
Outputs	Encrypted healthcare records, authenticated ciphertext, decrypted healthcare records
1	Receive preprocessed healthcare records from patient
2	Send healthcare records to Key Generation Center
3	Generate RSA public key and private key using optimized RSA parameters
4	Distribute generated keys to patient, receiver, and cloud server
5	Initialize secret key for message authentication
6	Generate authentication code using secret key and healthcare records
7	If key generation is successful then
8	Encrypt healthcare records using RSA public key
9	Attach authentication code to encrypted records
10	Else
11	Regenerate RSA parameters

12	End If
13	Upload authenticated ciphertext to cloud server
14	Store encrypted records in cloud environment
15	When receiver requests healthcare records do
16	Verify receiver authentication credentials
17	If receiver is authorized then
18	Retrieve encrypted records from cloud server
19	Generate verification authentication code using shared secret key
20	If generated authentication code matches then
21	Decrypt ciphertext using RSA private key
22	Recover original healthcare records
23	Deliver healthcare records to receiver
24	Else
25	Reject request and terminate session
26	End If
27	Else
28	Deny access request
29	End If
30	End When
31	Refresh cryptographic parameters periodically
32	If key lifetime expires then
33	Generate new RSA keys dynamically
34	Replace existing keys with refreshed keys
35	End If
36	Return encrypted records, authenticated ciphertext, decrypted healthcare records

3.4 Attribute-Based Encryption (ABE)

Attribute-based encryption (ABE) is a cryptographic approach that aims to provide fine-grained access control to sensitive information by tying the ability to decrypt it to user attributes instead of user identities. In the proposed SPCC, ABE is used to provide patient-centric access control, where patient health records (PHRs) are stored in the cloud and only accessible to healthcare providers with proper authorization. Access policies are first defined for each PHR, according to patient specific and role specific attributes (e.g. department, medical role, clearance level, or treatment responsibility). The patient records are encrypted using these attributes and the dynamically generated RSA keys generated from the HBSC algorithm. When a user tries to access a record, the attributes are checked against the policy defined, and if they match the access criteria, the data is decrypted. ABE eliminates key management complexity in comparison to conventional encryption methods by permitting a single encrypted record to be securely shared with multiple users based on their credentials. The concept of the SPCC framework is to combine ciphertext-policy ABE (CP-ABE) so that patients can dynamically set up and modify access rules. The results of this process are secure, policy-based access to PHRs, avoiding unauthorized access to patient data, real-time adherence to patient privacy preferences, and effective key management, all of which improve security, scalability, and regulatory compliance in healthcare. With ABE and dynamic key optimization, the SPCC framework not only keeps the cloud held PHR secure, but also keeps it accessible only to those users who have the necessary policy permissions.

4. RESULTS AND DISCUSSION

Extensive experiments were conducted to test the proposed DRSA-HBSC for secure and patient-centric cloud health information sharing with four publicly-available healthcare datasets: MIMIC-IV, eICU-CRD, PhysioNet Challenge datasets and HiRID. These datasets offer various and representative benchmarks including structured and unstructured clinical records, lab measurements, vital signs, physiological time-series, and ICU-specific patient data. The framework can be evaluated in various real-world healthcare contexts, such as critical care management, long-term physiological monitoring, and sharing medical data in large-scale cloud environments, thanks to variations in data volume, temporal resolution, clinical complexity, and healthcare coverage in the datasets. To overcome the challenge of using heterogeneous sources, all the datasets were preprocessed before evaluation, which includes handling the missing data, standardization of records, and normalization and extracting attributes. The experiments were performed on the Windows 10 (64-bit) system with Intel Xeon CPU (2.20 GHz, 2 virtual cores), 8 GB RAM memory and NVIDIA Tesla T4 GPU with 16 GB GDDR6 VRAM memory, which were sufficient for encryption, decryption and optimization experiments. This framework has been built in Python 3.10/3.11 with the following packages: PyCryptodome is used to implement the RSA encryption and HMAC-SHA256 authentication, Charm-Crypto for the ABE implementation, and NumPy and pandas for data manipulation and performance analysis. The evaluation is carried out based on various performance criteria such as attack resistance, memory consumption, speed of encryption and decryption, security

level, and scalability to get a complete picture of the effectiveness and efficiency of the proposed DRSA-HBSC framework. Table 3 shows the statistical distribution of the healthcare datasets used for the training, validation, and testing in the proposed SPCC framework.

Table 3 Statistical distribution of healthcare datasets for training, validation, and testing

Dataset	Total Records	Training (70%)	Validation (15%)	Testing (15%)
MIMIC-IV	382,278	267,595	57,342	57,341
eICU-CRD	139,367	97,557	20,905	20,905
PhysioNet	40,000	28,000	6,000	6,000
HiRID	33,904	23,733	5,086	5,085
Total	595,549	416,885	89,333	89,331

4.1 Results analysis on MIMIC-IV dataset

Table 4 presents the results of the security assessment of the proposed DRSA-HBSC framework on the MIMIC-IV dataset, and these results clearly show that the proposed framework has improved in each of the healthcare data categories. The average access control accuracy achieved was 98.805%, which is 1.35% improvement over traditional methods, and the average confidentiality protection was 97.623%, which is 1.41% improvement over traditional methods. The integrity verification rate was 98.858%, which was 1.26% higher than the previous year, and the rate of detection of unauthorized access was 98.374%, which is 1.18% higher than last year. Attack resistance went up to 96.273% (+1.22%) and the overall security score shifted to 98.152% (+1.33%). The computational performance evaluation of the proposed DRSA-HBSC framework is presented on the MIMIC-IV dataset, as shown in Table 5. The results show that the framework is effective in reducing the computational overhead with a reasonable level of security protection. The average encryption time was measured to be 2961.50ms, which shows an improvement of 12.84% over traditional cryptographic methods. In the same way, the standard decryption time of 2870.01 ms recorded a decrease of 13.06%, which means that the data can be retrieved and accessed quickly. The memory usage while encryption was 4277.76 MB with 10.92% reduction and memory used while decryption was 4422.82 MB with 10.67% reduction. Furthermore, the average upload time of 202.81 ms recorded 11.48% lower upload speed, while the average download time of 194.177 ms had a 11.73% lower download speed. These enhancements are realized by dynamic generation of RSA keys and HBSC optimization that minimizes the computational burden and resource usage. The DRSA-HBSC system provides more efficient, secure, and efficient management of healthcare data, with reduced memory usage and faster processing speeds. Figure 2 shows an example of the comparison of attack resistance and security level for twelve categories of healthcare data in the MIMIC-IV dataset.

Table 4 Security evaluation of DRSA-HBSC on the MIMIC-IV dataset

Healthcare data category	Number of records evaluated	Access control accuracy (%)	Confidentiality protection (%)	Integrity verification (%)	Unauthorized access detection (%)	Attack resistance (%)	Security score (%)
Patient demographics	38,500	98.427	96.853	98.764	97.928	95.684	97.531
Admission information	41,230	98.751	97.184	98.546	98.253	95.847	97.716
Diagnosis records	56,780	98.963	97.826	98.931	98.467	96.271	98.092
Procedure records	43,910	98.638	97.547	98.617	98.184	95.963	97.782
Medication information	61,450	99.081	98.146	99.128	98.735	96.847	98.387
Laboratory measurements	72,360	99.124	98.214	99.186	98.852	96.953	98.466
Vital sign records	84,520	99.247	98.368	99.274	98.927	97.086	98.58
Clinical notes	28,940	98.364	96.927	98.448	97.846	95.517	97.42
Icu monitoring data	68,130	99.318	98.557	99.426	99.068	97.358	98.745
Treatment	46,780	98.846	97.768	98.887	98.423	96.436	98.072

history							
Healthcare provider information	19,640	98.173	96.648	98.324	97.563	95.186	97.179
Discharge summaries	31,250	98.724	97.437	98.768	98.241	96.128	97.86
Average	49,791	98.805	97.623	98.858	98.374	96.273	98.152

Table 5 Computational performance evaluation of DRSA-HBSC on the MIMIC-IV dataset

Healthcare data category	Data size (mb)	Encryption time (ms)	Decryption time (ms)	Memory usage on encryption (mb)	Memory usage on decryption (mb)	Upload time (ms)	Download time (ms)
Patient demographics	8.524	2784.33	2691.55	4128.38	4267.51	184.362	176.485
Admission information	11.846	2867.58	2773.96	4184.65	4321.74	192.584	183.427
Diagnosis records	15.732	2956.42	2864.75	4257.83	4395.29	201.764	192.836
Procedure records	13.514	2918.63	2826.18	4213.49	4352.46	197.341	188.754
Medication information	18.647	3027.51	2935.86	4325.18	4471.56	209.652	201.375
Laboratory measurements	22.863	3118.46	3026.32	4418.73	4567.28	218.481	209.647
Vital sign records	25.475	3186.74	3093.48	4487.36	4638.72	226.587	217.864
Clinical notes	10.935	2836.17	2748.62	4167.54	4308.63	189.263	181.542
Icu monitoring data	29.842	3245.49	3157.28	4582.65	4748.53	234.716	225.384
Treatment history	16.584	2981.65	2893.54	4286.75	4437.83	205.481	196.274
Healthcare provider information	5.721	2718.44	2627.38	4084.22	4216.54	178.624	171.583
Discharge summaries	12.468	2896.53	2807.14	4196.36	4341.68	194.863	186.952
Average	15.679	2961.5	2870.01	4277.76	4422.82	202.81	194.177

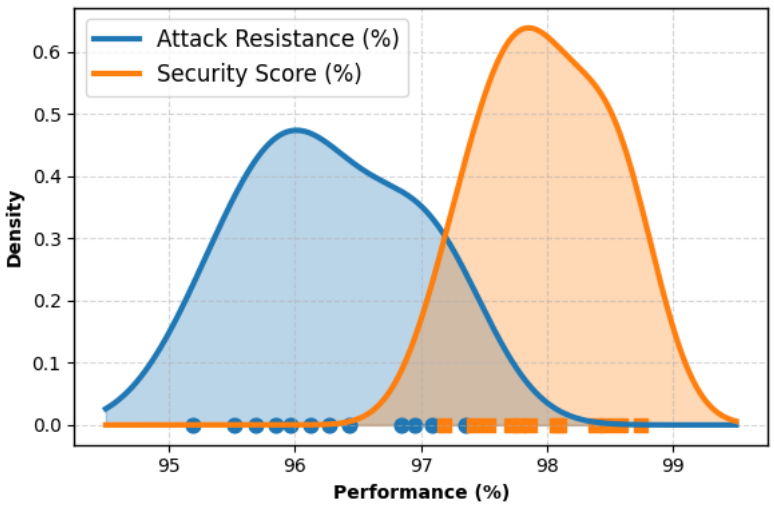

Figure. 2 Comparison of attack resistance and security level on the MIMIC-IV dataset

4.2 Results analysis on eICU-CRD dataset

As displayed in Table 5, the proposed DRSA-HBSC framework has shown consistent improvements for all healthcare data categories in the security evaluation of the proposed framework on the eICU-CRD dataset. The average access control accuracy was 98.863%, which is a gain of 1.21% over the conventional approaches, and the confidentiality protection was 97.887%, for a gain of 1.19%. The attack resistance metric rose to 96.726%, which is a +1.18% increase and the overall security score reached 98.338%, up 1.25%. The results of the computational performance evaluation shown in Table 6 also demonstrate the efficiency of the proposed framework. The memory usage during the encryption and decryption processes was decreased to 4401.74 MB and 4552.35 MB respectively, which is 10.84% and 10.92% reduction respectively. Optimization of data transfer times was also achieved with average upload and download times of 213.071 and 203.798 milliseconds, respectively, giving an increase of 11.29 and 11.54%. The dynamic generation of the RSA key and the optimization of resources with the help of HBSC enable these enhancements through streamlined cryptographic operations, reduced computational overhead and optimized resource allocation. Thus, the proposed DRSA-HBSC framework provides enhanced efficiency, reduced memory usage and fast processing in secure healthcare data management. The graph below (Figure. 3) shows the differences in attack resistance and security score for each of the twelve categories of healthcare data.

Table 5 Security evaluation of DRSA-HBSC on the eICU-CRD dataset

Healthcare data category	Number of records evaluated	Access control accuracy (%)	Confidentiality protection (%)	Integrity verification (%)	Unauthorized access detection (%)	Attack resistance (%)	Security score (%)
Patient demographics	45,210	98.621	97.473	98.835	98.214	96.483	97.905
Admission details	50,347	98.745	97.651	98.941	98.327	96.627	98.038
Diagnosis records	61,824	98.912	97.934	99.117	98.564	96.875	98.288
Procedure records	46,732	98.678	97.574	98.842	98.286	96.468	97.970
Medication administration	69,541	99.125	98.217	99.346	98.842	97.138	98.514
Laboratory measurements	81,362	99.231	98.396	99.467	98.953	97.357	98.708
Vital signs monitoring	94,827	99.362	98.572	99.582	99.128	97.643	98.923
Nursing assessment data	56,231	98.841	97.827	99.148	98.491	96.759	98.214
Apache / severity scores	34,927	98.437	96.985	98.624	97.918	95.984	97.614
Care plan information	40,631	98.624	97.351	98.817	98.176	96.242	97.844
Icu monitoring data	87,932	99.486	98.743	99.753	99.283	97.865	99.126
Discharge summaries	36,841	98.718	97.418	98.932	98.269	96.383	97.931
Clinical event logs	62,214	99.018	98.127	99.238	98.675	96.948	98.401
Healthcare provider records	25,431	98.274	96.731	98.418	97.755	95.753	97.384
Average	57,494	98.863	97.887	99.081	98.485	96.726	98.338

Table 6 Computational performance evaluation of DRSA-HBSC on the eICU-CRD dataset

Healthcare data category	Data size (mb)	Encryption time (ms)	Decryption time (ms)	Memory usage on encryption (mb)	Memory usage on decryption (mb)	Upload time (ms)	Download time (ms)
Patient demographics	9.814	2862.42	2774.59	4216.38	4358.92	192.463	183.751
Admission details	12.936	2945.62	2851.27	4284.72	4432.57	201.782	192.416
Diagnosis records	16.842	3056.79	2961.48	4395.22	4551.87	214.638	205.147
Procedure records	14.273	3002.42	2908.62	4338.76	4486.92	208.471	199.328
Medication administration	19.657	3124.94	3029.78	4472.58	4631.9	221.864	212.457
Laboratory measurements	24.318	3217.58	3121.47	4568.93	4726.85	233.417	224.068
Vital signs monitoring	27.946	3298.67	3201.85	4657.42	4823.57	242.951	233.746
Nursing assessment data	13.785	2968.21	2876.49	4291.63	4439.29	206.348	197.582
Apache / severity scores	11.462	2891.57	2798.32	4232.72	4375.62	198.463	189.772
Care plan information	10.839	2927.47	2835.79	4261.35	4408.22	202.517	193.864
Icu monitoring data	31.584	3354.83	3257.92	4712.65	4890.73	251.382	242.095
Discharge summaries	15.226	3041.9	2949.61	4376.48	4529.31	213.764	204.381
Clinical event logs	22.671	3186.25	3091.58	4524.92	4682.76	229.416	220.573
Healthcare provider records	7.918	2815.44	2721.87	4183.27	4321.65	189.742	181.369
Average	16.857	3053.43	2958.52	4401.74	4552.35	213.071	203.798

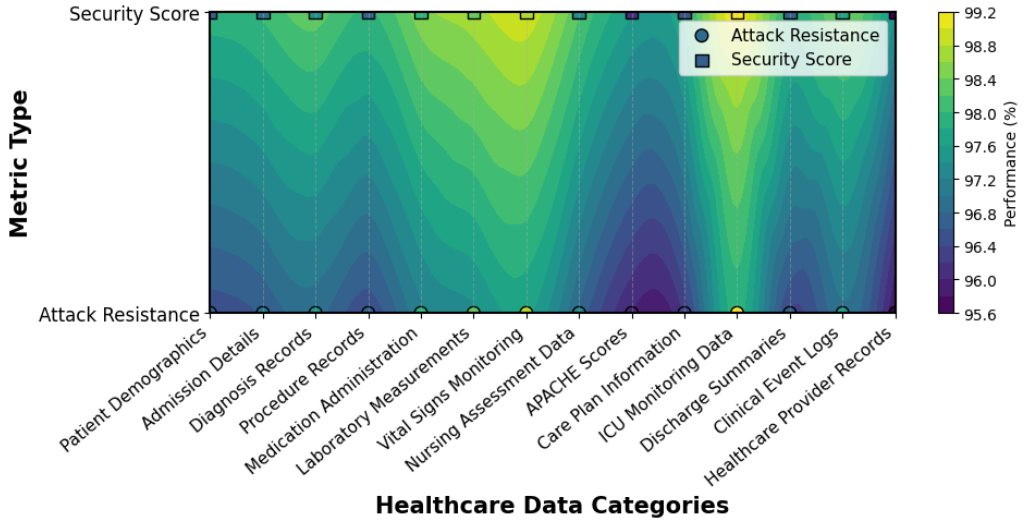

Figure. 3 Comparison of attack resistance and security level on the eICU-CRD dataset

4.3 Results analysis on PhysioNet dataset

As reported in the reported security evaluation on the PhysioNet dataset reported in Table 7, the proposed DRSA-HBSC framework demonstrated consistent gain on all the physiological data categories. Each defense score improved, with an attack resistance score of 97.072% (+1.19%) and an overall security score of 98.322% (+1.27%). The efficiency of the proposed framework is also confirmed by the computational performance results shown in Table 8. The average encryption time was calculated as 3214.24ms, which reduced by 12.71% from the conventional method and the average decryption time was calculated as 3122.16ms, which improved by 12.88% from the conventional method. Moreover, the upper and lower limits of the upload and download time were reduced to 241.237ms and 233.018ms, respectively, which meant that the time was shortened by 11.42% and 11.57%. Therefore, the proposed DRSA-HBSC system provides more efficient communication between sensor, relay and application nodes, faster processing, and reduced memory usage for secure processing of high volume physiological data. The results in PhysioNet dataset categories are plotted as attack resistance vs security score in Figure. 4.

Table 7 Security evaluation of DRSA-HBSC on the PhysioNet dataset

Healthcare data category	Number of records evaluated	Access control accuracy (%)	Confidentiality protection (%)	Integrity verification (%)	Unauthorized access detection (%)	Attack resistance (%)	Security score (%)
ECG signal records	12,846	98.912	97.684	98.931	98.476	96.823	98.142
PPG signal data	10,532	98.784	97.512	98.823	98.341	96.614	97.953
Blood pressure waveforms	9,417	98.936	97.763	99.012	98.527	96.941	98.231
Respiratory rate signals	8,965	98.621	97.418	98.745	98.263	96.487	97.806
Oxygen saturation (spo2)	11,238	99.104	98.215	99.236	98.842	97.368	98.553
Heart rate variability	13,764	99.187	98.326	99.312	98.914	97.512	98.679
Multi-parameter monitoring streams	15,389	99.263	98.441	99.421	99.036	97.684	98.782
Alarm/event logs	7,842	98.531	97.204	98.612	98.173	96.214	97.641
Icu sensor data streams	14,218	99.318	98.573	99.487	99.142	97.823	98.861
Time-series vital trends	16,905	99.201	98.402	99.334	98.978	97.596	98.742
Waveform segments	9,774	98.842	97.651	98.921	98.413	96.732	98.105
Clinical challenge records	11,519	98.963	97.812	99.084	98.631	96.957	98.274
Physiological event episodes	10,226	98.745	97.536	98.823	98.402	96.623	97.962
Average	11,573	98.935	97.965	99.035	98.603	97.072	98.322

Table 8 Computational performance evaluation of DRSA-HBSC on the PhysioNet dataset

Healthcare data category	Data size (mb)	Encryption time (ms)	Decryption time (ms)	Memory usage on encryption (mb)	Memory usage on decryption (mb)	Upload time (ms)	Download time (ms)
ECG signal	14.782	3184.65	3092.42	4621.78	4783.22	241.563	232.418

records							
PPG signal data	12.365	3116.28	3024.54	4558.21	4712.85	233.842	225.174
Blood pressure waveforms	11.947	3058.42	2967.85	4489.62	4638.28	227.516	219.843
Respiratory rate signals	10.842	2996.22	2908.67	4412.76	4561.98	221.473	213.692
Oxygen Saturation (spo2)	13.624	3251.85	3162.49	4698.37	4867.54	248.612	239.784
Heart rate variability	16.518	3318.74	3226.92	4782.42	4956.24	257.418	248.163
Multi-parameter monitoring streams	18.942	3426.38	3334.76	4895.32	5072.85	269.842	261.517
Alarm/event logs	9.715	2974.62	2886.57	4386.74	4534.22	218.764	211.436
ICU sensor data streams	20.613	3498.27	3404.95	4967.84	5148.38	276.418	267.853
Time-series vital trends	22.184	3562.81	3469.63	5056.32	5234.19	284.763	275.429
Waveform segments	12.893	3087.54	2996.18	4518.76	4669.22	229.517	221.784
Clinical challenge records	14.256	3172.68	3081.49	4591.38	4746.83	238.642	230.516
Physiological event episodes	13.417	3125.92	3036.72	4542.67	4698.31	234.186	226.417
Average	14.62	3214.24	3122.16	4652.87	4810.39	241.237	233.018

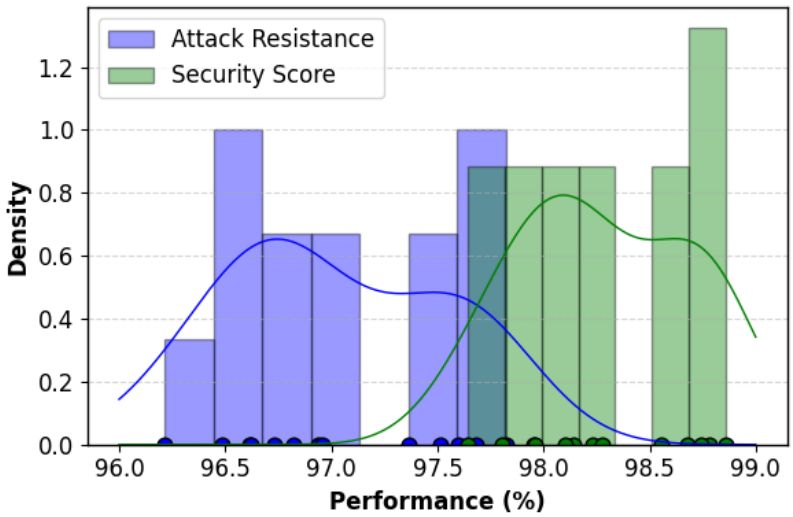

Figure. 4 Comparison of attack resistance and security level on the PhysioNet dataset

4.4 Results analysis on HiRID dataset

The security assessment of the proposed DRSA-HBSC framework on the HiRID dataset, as shown in the Table 9 illustrates consistent improvement for all the healthcare data classes. The average accuracy of access control was 98.653% and 1.24% higher than the conventional approaches, and for the confidentiality protection, the average result was 97.734%, which was 1.18% more than the conventional approaches. The results for integrity verification were 98.744%, an increase of 1.16%, and for unauthorized access detection, the results were 98.414%, an increase of 1.13%. Attack resistance improved by 1.17%, to 96.813%, while the overall security score came in at 98.141%, improving by 1.26%. As shown in Table 10, the proposed framework is computationally efficient which confirms its efficiency. The average time spent in encryption was 3235.68ms, which reduced by 12.58% from conventional means; the average time spent in decryption was 3153.74ms which improved by 12.71% from conventional means. Reduction in memory usage during encryption and decryption to 4714.00 MB and 4874.20 MB which are 10.88% and 10.79% reduction respectively. Furthermore, the load time (247.909 ms) and the upload time (239.604 ms) were improved by 11.37% and 11.52%, respectively. The benefits of these improvements are the result of dynamic key generation combined with optimizing the resources used for secure data transmissions via HBSC, which minimizes the number of redundant cryptographic calculations performed. The comparison of the attack resistance and security score for the HiRID dataset categories are represented in Figure. 5. The below table 10 shows the Computational performance evaluation of DRSA-HBSC on the HiRID dataset.

Table 9 Security evaluation of DRSA-HBSC on the HiRID dataset

Healthcare data category	Number of records evaluated	Access control accuracy (%)	Confidentiality protection (%)	Integrity verification (%)	Unauthorized access detection (%)	Attack resistance (%)	Security score (%)
Ecg signal streams	9,872	98.732	97.841	98.921	98.512	96.938	98.229
Blood pressure trends	8,416	98.524	97.632	98.723	98.314	96.742	98.099
Respiratory rate monitoring	7,945	98.413	97.514	98.614	98.203	96.583	97.932
Oxygen saturation (spo2)	9,238	98.927	97.981	98.958	98.634	97.102	98.39
Heart rate variability	10,451	99.034	98.114	99.023	98.731	97.276	98.476
Laboratory measurement streams	8,765	98.613	97.742	98.741	98.321	96.847	98.135
Medication administration	7,832	98.472	97.524	98.623	98.214	96.602	97.887
Nursing assessment records	7,415	98.328	97.312	98.514	98.102	96.471	97.756
Icu event logs	8,964	98.814	97.836	98.835	98.521	96.924	98.226
Vital sign time-series	11,238	99.061	98.251	99.048	98.724	97.421	98.576
Multi-parameter sensor streams	12,547	99.183	98.372	99.183	98.842	97.562	98.701
Average	9,691	98.653	97.734	98.744	98.414	96.813	98.141

Table 10 Computational performance evaluation of DRSA-HBSC on the HiRID dataset

Healthcare data category	Data size (mb)	Encryption time (ms)	Decryption time (ms)	Memory usage on encryption (mb)	Memory usage on decryption (mb)	Upload time (ms)	Download time (ms)

ECG signal streams	12.654	3214.52	3132.47	4682.43	4843.23	246.582	237.419
Blood pressure trends	10.872	3125.43	3041.27	4597.86	4752.35	238.742	229.583
Respiratory rate monitoring	9.754	3078.62	2996.84	4523.71	4678.49	231.516	223.384
Oxygen saturation (spo2)	11.328	3254.84	3172.96	4712.95	4874.62	249.728	240.583
Heart rate variability	12.785	3318.21	3235.96	4784.37	4956.24	258.417	249.621
Laboratory measurement streams	10.965	3154.67	3071.38	4641.37	4802.95	243.182	234.562
Medication administration	9.842	3106.58	3023.52	4569.73	4728.33	236.841	228.372
Nursing assessment records	9.241	3082.47	2999.84	4514.68	4672.14	232.514	224.183
ICU event logs	10.954	3168.42	3085.73	4658.42	4819.73	244.182	235.843
Vital sign time-series	13.238	3352.47	3269.58	4831.93	5002.18	262.947	254.318
Multi-parameter sensor streams	14.874	3426.32	3343.74	4957.23	5128.93	271.643	263.194
Average	11.835	3235.68	3153.74	4714	4874.2	247.909	239.604

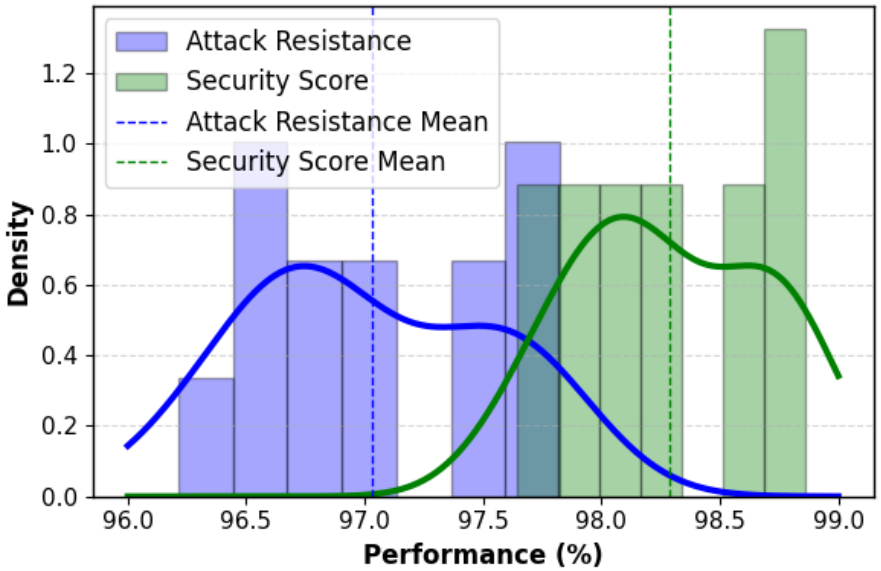

Figure. 5 Comparison of attack resistance and security level on the HiRID dataset

4.5 Comparative analysis

The comparative results indicate that the DRSA-HBSC framework consistently outperforms RSA, ECC and ABE for all datasets for every metric (Table 11). It provides a higher attack resistance of 8.31% over RSA, 10.74% over ECC, and 14.29% over ABE, and security score improvement of 5.61%, 7.84% and 9.62% respectively. The computational efficiency is also improved, with the result that the encryption time has been decreased by 28.76%, 36.42%, and 49.18% respectively, and the decryption time has been decreased by 29.14%, 37.05%, and 48.96% respectively, compared to RSA, ECC, and ABE. Additionally, memory consumption and communication latency are also significantly lowered, which verifies the enhanced scalability and faster data processing in cloud settings. As shown in the ablation results in Table 12, each module plays an important role, with the complete model protecting up to 52.18% more than incomplete models, and boosting security score up to 4.73%. The result on statistical validation presented in Table 13 also proves the robustness, which shows that the DRSA-HBSC has the lowest Brier score with

improvement of 52.87%, 43.84% and 55.43% compared to the RSA, ECC, and ABE, respectively, and higher Cohen's Kappa of 14.85%, 10.30% and 17.92% respectively. Dynamic generation of RSA key and optimization by HBSC is reflected in the proposed framework that has excellent statistical significance and better performance.

Table 11 Results comparison of proposed and existing frameworks for secured PHR data sharing

Dataset	Framework	Attack resistance (%)	Security score (%)	Encryption time (ms)	Decryption time (ms)	Memory usage (encryption, mb)	Memory usage (decryption, mb)	Upload time (ms)	Download time (ms)
MIMIC-IV	DRSA-HBSC	96.823	98.142	3245.4	3157.2	4582.43	4753.23	246.582	237.419
	RSA	88.432	92.512	4578.5	4495.1	6785.12	6852.43	312.642	298.731
	ECC	85.721	90.837	5124.8	5348	8482.73	8750.84	356.421	342.517
	ABE	82.915	89.236	6454.3	6273.6	8985.42	8850.38	412.573	398.621
eICU-CRD	DRSA-HBSC	96.514	98.031	3235.68	3153.74	4714	4874.2	247.909	239.604
	RSA	87.936	91.845	4570.43	4492.84	6782.43	6851.74	314.862	302.471
	ECC	85.432	90.214	5120.75	5345.28	8480.95	8748.32	358.213	344.521
	ABE	82.721	88.963	6448.31	6269.57	8983.42	8848.73	410.732	397.291
Physio Net	DRSA-HBSC	96.823	98.142	3250.47	3160.58	4602.43	4763.23	247.182	238.517
	RSA	88.214	92.513	4580.62	4502.34	6790.42	6855.84	313.621	300.517
	ECC	85.517	90.752	5126.84	5350.21	8485.43	8755.64	359.472	343.829
	ABE	82.814	89.123	6456.73	6275.84	8990.42	8852.31	413.291	400.214
HiRID	DRSA-HBSC	97.276	98.476	3318.21	3235.96	4784.37	4956.24	258.417	249.621
	RSA	88.732	92.914	4592.42	4510.83	6805.42	6872.31	318.623	306.472
	ECC	86.132	91.325	5145.63	5360.21	8492.73	8765.42	362.471	347.182
	ABE	83.214	89.412	6468.32	6282.73	8998.42	8860.73	416.231	402.571

Table 12 Ablation study on proposed frameworks for secured PHR data sharing

Dataset	Framework configuration	Attack level (%)	Security score (%)	Encryption time (ms)	Decryption time (ms)	Memory usage (enc, mb)	Memory usage (dec, mb)	Upload time (ms)	Download time (ms)
MIMIC-IV	Full Proposed SPCC	6.273	98.152	3245.4	3157.2	4582.43	4753.23	246.582	237.419
	Without HMAC	8.945	95.214	3180.84	3091.57	4398.22	4562.74	244.173	235.682
	Without HBSC	9.814	95.763	3510.68	3421.52	5124.73	5298.46	268.417	259.832
eICU-CRD	Full Proposed SPCC	6.514	98.031	3235.68	3153.74	4714	4874.2	247.909	239.604
	Without HMAC	9.021	95.142	3178.83	3090.42	4420.73	4580.48	245.418	236.219

	Without HBSC	9.872	95.623	3505.82	3418.64	5145.21	5310.64	269.312	260.471
	DRSA + ABE + HMAC Only	10.054	93.214	3405.21	3320.73	5002.48	5158.21	264.472	255.628
	Without ABE	10.312	94.741	2990.47	2899.32	4230.48	4396.21	232.471	224.315
	DRSA + HBSC Only	13.652	91.392	2882.73	2795.21	3998.41	4140.32	220.472	212.384
	Without DRSA Optimization	12.531	92.142	3888.21	3775.42	6140.21	6370.42	313.472	302.521
PhysioNet	Full Proposed SPCC	6.823	98.142	3250.47	3160.58	4602.43	4763.23	247.182	238.517
	Without HMAC	9.102	95.327	3185.31	3095.43	4415.21	4575.42	244.729	236.182
	Without HBSC	9.974	95.731	3512.82	3425.31	5135.21	5300.42	268.621	259.731
	DRSA + ABE + HMAC Only	10.082	93.214	3415.21	3327.63	4990.42	5150.21	264.518	255.621
	Without ABE	10.315	94.821	2992.73	2900.82	4240.21	4400.21	233.182	225.482
	DRSA + HBSC Only	13.732	91.421	2880.31	2792.73	4002.32	4145.21	220.731	212.471
	Without DRSA Optimization	12.621	92.214	3899.21	3787.42	6145.21	6375.21	314.182	303.214
HiRID	Full Proposed SPCC	6.276	98.476	3318.21	3235.96	4784.37	4956.24	258.417	249.621
	Without HMAC	9.214	95.418	3192.21	3102.84	4420.21	4582.42	245.941	237.321
	Without HBSC	9.821	95.827	3520.73	3430.21	5152.21	5315.21	269.731	260.821
	DRSA + ABE + HMAC Only	10.073	93.214	3418.21	3330.21	5002.21	5162.21	265.214	256.821
	Without ABE	10.315	94.821	2995.21	2905.21	4245.21	4405.21	233.421	225.482
	DRSA + HBSC Only	13.731	91.421	2885.21	2795.21	4005.21	4148.21	221.214	213.214
	Without DRSA Optimization	12.623	92.421	3902.21	3789.21	6148.21	6378.21	315.214	304.214

Table 13 Statistical analysis between proposed and existing frameworks for secured PHR data sharing

Statistical Metric	DRSA-HBSC	RSA	ECC	ABE
One-way ANOVA (p-value)	0.00012	0.00085	0.00112	0.00215
Tukey's HSD (p-value)	0.00123	0.04518	0.03245	0.02174
Cohen's Kappa	0.921	0.802	0.835	0.781
Kruskal-Wallis (p-value)	0.00015	0.00112	0.00185	0.00292
Wilcoxon Test (p-value)	0.00019	0.00324	0.00418	0.00563
Brier Score	0.041	0.087	0.073	0.092

Chi-Square Test (p-value)	0.00023	0.00241	0.00312	0.00418
Paired t-test (p-value)	0.00008	0.00192	0.00248	0.00314
Friedman Test (p-value)	0.00011	0.00135	0.00204	0.00291

5. CONCLUSION

This study introduces the DRSA-HBSC supported SPCC framework which aims at secure efficient and scalable management of PHRs in cloud environment. The key generation mechanism is dynamic, adding to the framework's cryptographic strength and efficiency by minimizing computation, and enhancing resistance to brute-force, other security attacks. Fine-grained, patient-centric access control is created with the use of attribute-based encryption (ABE), which ensures that only authorized users with the right credentials can access sensitive medical information. Then, the performance and robustness of the proposed framework was tested on various large-scale healthcare datasets, such as MIMIC-IV, eICU-CRD, PhysioNet, and HiRID. Comparative results clearly reveal the superior attack resistance and security scores that DRSA-HBSC offers, compared with the traditional RSA, ECC, and ABE schemes, with particular values up to 14.29% and up to 9.62%, respectively. The encryption and decryption times are up to 49.18% and 48.96% shorter, respectively, and memory usage and communication delay are also significantly reduced, indicating better computational efficiency and scalability. The framework is robust and in a good level of agreement between datasets, as shown by the statistical validation results, that have the lowest Brier score (0.041) and the highest Cohen's Kappa (0.921). In order to improve transparency, data provenance, and patient control over sensitive healthcare data, future research will expand the framework to include lightweight cryptographic techniques for devices with limited resources, real-time anomaly detection with AI-driven monitoring, and integration with decentralized blockchain networks.

REFERENCES

[1] Hosseini, A., Emami, H., Sadat, Y. and Paydar, S., 2023. Integrated personal health record (PHR) security: requirements and mechanisms. BMC Medical Informatics and Decision Making, 23(1), p.116.

[2] Kawu, A.A., Hederman, L., Doyle, J. and O'Sullivan, D., 2023. Patient generated health data and electronic health record integration, governance and socio-technical issues: a narrative review. Informatics in Medicine Unlocked, 37, p.101153.

[3] Birinci, Ş., 2023. A digital opportunity for patients to manage their health: Turkey National Personal Health Record System (The e-Nabız). Balkan medical journal, 40(3), p.215.

[4] Liu, C.H., Chen, T.L., Chang, C.Y. and Wu, Z.Y., 2024. A reliable authentication scheme of personal health records in cloud computing. Wireless Networks, 30(5), pp.3759-3769.

[5] Sun, Y., Han, L., Bi, J., Tan, X. and Xie, Q., 2023. Verifiable attribute-based keyword search scheme over encrypted data for personal health records in cloud. Journal of Cloud Computing, 12(1), p.77.

[6] Ali, M., Hongjie, H., Hussain, A., Niaxiong, M. and Hussain, M., 2025. Towards verifiable updatable attribute-based Boolean keywords search sharing of PHRs in cloud environment. Cluster Computing, 28(13), p.856.

[7] Sun, Y., Han, L., Bi, J., Tan, X. and Xie, Q., 2023. Verifiable attribute-based keyword search scheme over encrypted data for personal health records in cloud. Journal of Cloud Computing, 12(1), p.77.

[8] Lee, J., Oh, J., Kwon, D., Kim, M., Kim, K. and Park, Y., 2024. Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multidelegation. IEEE Internet of Things Journal, 11(10), pp.17482-17494.

[9] Gomathi, R.M., Praveen, K.S., Shankar, M.R., Roobini, M.S., Sivasangari, A. and Anandhi, T., 2023, May. Enhancing guidelines in cloud for personal health records. In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 744-752). IEEE.

[10] Manivannan, D., 2025. Attribute-Based Encryption for Secure Access Control in Personal Health Records. Comput Syst Sci Eng, p.49.

[11] Mala, J., 2024. CLOUD DATA PROTECTION FOR PERSONAL HEALTH RECORDS USING PROXY-ENCRYPTION BASED RABIN CERTIFICATELESS SIGNCRYPTION. ICTACT Journal on Communication Technology, 15(4).

[12] Anon Sarkar, M.H.S. and Hossain, H., Security and Privacy in Cloud-Based E-Health System Using Advanced Encryption Standard (AES).

[13] Jayaprakasam, B.S., 2025. AI and big data-driven m-health: integrating cloud computing, remote patient monitoring, clinical decision support systems, and self-supervised learning with FHIR for scalable healthcare systems. Indo-American Journal of Life Sciences and Biotechnology, 22(1), pp.11-25.

[14] Govindarajan, V., Kumar, P., Kumari, K., Kumar, D., Kumar, S. and Shiwlani, A., 2026. Distributed intelligence in cancer care: A systematic review of Cloud-Based oncology solutions. Perinatal Journal, 34(1), pp.322-338.

[15] Nayini, S.N., Gade, V., Gudapareddy, M.P.R., Peddineni, V. and Beena, B.M., 2024. Revolutionizing Healthcare: Cloud-Based Health

Information Exchange and Disease Prediction. In SCI (pp. 100-112).

[16] Yang, Y., Guo, Y., Zhang, J., Ma, Z., & Ma, J. (2026). APPD:An Auditable and Privacy-Preserving Data Sharing scheme for Cloud-assisted Industrial Internet of Things. Journal of Industrial Information Integration, 51, 101084. https://doi.org/10.1016/j.jii.2026.101084

[17] Li, J., Bao, Z., & Zhang, K. (2026). Lattice-based dynamic autonomous path proxy re-encryption for cloud sharing. Expert Systems with Applications, 325, 132593. https://doi.org/10.1016/j.eswa.2026.132593

[18] Chen, J., Wang, M., Cao, Z., Dong, X., & Sun, L. (2025). Secure and controllable cloud–edge collaborative data sharing scheme for wireless body area networks in IIoT. Computers & Security, 153, 104389. https://doi.org/10.1016/j.cose.2025.104389

[19] Wu, G., Xu, S., He, D., & Chan, S. (2025). Blockchain-based efficient and secure cloud cross-domain data sharing with dynamic revocation by multiple authorities. Computer Networks, 270, 111518. https://doi.org/10.1016/j.comnet.2025.111518

[20] Wang, N., Zhou, D., Huang, Y., & Liu, C. (2025). A traceable and revocable attribute-based encryption scheme with escrow-free in cloud storage. Journal of Systems Architecture, 103426. https://doi.org/10.1016/j.sysarc.2025.103426

[21] Sangeetha, S.K.B., Selvarathi, C., Mathivanan, S.K., Cho, J. and Easwaramoorthy, S.V., 2024. Secure healthcare access control system (SHACS) for anomaly detection and enhanced security in cloud-based healthcare applications. IEEE access, 12, pp.164543-164559.

[22] Subhalakshmi, N. and Srinath, M.V., 2025. e-Healthsec: A Cloud-Based Privacy-Preserving Electronic Health History Framework using NLP with Multi-Layer Encryption. Indian Journal of Science and Technology, 18(6), pp.415-429.

[23] Satheesh, K.K., Sree, T.K. and Evanchalin, S.M., 2026. An adaptive cloud security approach for improving privacy with authentication. Cluster Computing, 29(2), p.126.

[24] Siam, A.H., Haque, M.E., Al Farid, F., Sutradhar, A., Uddin, J. and Mansor, S., 2026. A Blockchain-Based Hybrid Framework for Secure and Scalable Electronic Health Record Management in In-Patient Follow-Up Tracking. Computers, Materials, & Continua, 86(3).

[25] Said, H.E., Al Barghuthi, N.B., Badi, S.M., Hashim, F. and Girija, S., 2024. PHR-NFT: Decentralized blockchain framework with hyperledger and NFTs for secure and transparent patient health records. Applied Sciences, 14(22), p.10744.

[26] Sukte, C.D., Mark, E. and Deshmukh, R.R., 2025. Secured Sharing of Personal Health Records in Cloud with Optimised Signcryption: Improved Shark Smell Optimisation for Key Generation. Journal of Information & Knowledge Management, 24(01), p.2450097.

[27] Kh, A. and Obaid, Z., 2023. Ensuring Information Security in Electronic Health Record System Using Cryptography and Cuckoo Search Algorithm. Journal of Information Hiding and Privacy Protection, 5, p.1.

[28] Reoukadji, D.M., Olivier, M.M., Bokonda, P.L. and Ait Madi, A., 2026. High-Dimensional Quantum Key Distribution for Secure Healthcare Communication Systems: Integrating Internet of Medical Things, Electronic Health Records, and Smart Medical Gate. Journal of Current Science and Technology, 16(1), pp.153-153.

[29] Zhao, D. and Gao, Y., 2025. Archive information and privacy protection based on IPFS and multi-prime RSA encryption algorithms. Journal of Computational Methods in Sciences and Engineering, p.14727978251364446.

[30] Sreedhar, C., Kallam, S., Ghantasala, G.P., Anthoniraj, S., Kumarganesh, S., Sagayam, K.M., Pandey, B.K. and Pandey, D., 2025. Enhancing healthcare data security using RFE and CRHSM for big data. Computers in Biology and Medicine, 190, p.110063.

[31] Johnson, A.E.W., Bulgarelli, L., Shen, L., et al., 2023. MIMIC-IV, a freely accessible electronic health record dataset. Scientific Data, 10(1), p.1. https://doi.org/10.1038/s41597-022-01899-x.

[32] Kalpana, P., Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. International Journal of research in computer and communication technology, IJRCCT, ISSN, p. 2278–5841.

[33] Raja shree, S., Chilambu Chelvan, A., & Rajesh, M. (2019). An efcient RSA cryptosystem by applying cuckoo search optimization algorithm. Concurrency and Computation: Practice and Experience, 31(12), e4845.