IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 March 2023, accepted 3 April 2023, date of publication 10 April 2023, date of current version 18 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3265954

RESEARCH ARTICLE

A Multi-Objective Bee Foraging Learning-Based Particle Swarm Optimization Algorithm for Enhancing the Security of Healthcare Data in Cloud System

REYAZUR RASHID IRSHAD[1], SHAHAB SAQUIB SOHAIL[2], SHAHID HUSSAIN[3], DAG ØIVIND MADSEN[4], MOHAMMED ALTAF AHMED[5], AHMED ABDU ALATTAB[1,6], OMAR ALI SALEH ALSAIARI[1], KHALID AHMED ABDALLAH NORAIN[1], AND ABDALLAH AHMED ALZUPAIR AHMED[1]

[1]Department of Computer Science, College of Science and Arts Sharoura, Najran University, Najran 55461, Saudi Arabia
[2]Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi 110062, India
[3]Innovative Value Institute, School of Business, Maynooth, W23 A023 Ireland
[4]USN School of Business, University of South-Eastern Norway, 3511 Hønefoss, Norway
[5]Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[6]Department of Computer Science, Faculty of Computer Science and Information Systems, Thamar University, Dhamar, Yemen

Corresponding authors: Shahab Saquib Sohail (shahabssohail@jamiahamdard.ac.in) and Dag Øivind Madsen (dag.oivind.madsen@usn.no)

This work was supported by the Deanship of Scientific Research at Najran University through the Research Groups Funding Program under Grant NU/RG/SERC/11/4.

ABSTRACT Cloud computing is a potential platform transforming the health sector by allowing clinicians to monitor patients in real-time using sensor technologies. However, the users tend to transmit sensitive and classified medical data back and forth to cloud service providers for centralized processing and storage. This presents opportunities for hackers to steal data, intercept data in transit, and deprive patients and healthcare providers of private information. Consequently, Security and privacy are the primary concerns that must be addressed for the healthcare organization to trust and adopt the cloud computing platform. We present data sanitization and restoration processes to generate the keys from the acquired data and develop a multi-objective function for the hiding ratio, degree of modification, and information preservation ratio. We then employed the Bee-Foraging Learning-based Particle Swarm Optimization (BFL-PSO) algorithm to acquire the optimal key while transferring healthcare data into the cloud to ensure high Security. The experiment is carried out on the UHDDS dataset. The performance is assessed in terms of Security, delay time, encryption time, error rate, and convergence speed, with the results contrasted to state-of-the-art works. The performance study demonstrates that the suggested algorithm has higher Security than cutting-edge security algorithms.

INDEX TERMS Healthcare, BFL-PSO, sanitization, restoration, cloud storage, degree of modification, hiding ratio, information preservation ratio.

I. INTRODUCTION

Cloud computing offers distributed database, networking, storage, data analysis, and Internet of Things (IoT) services to various stakeholders, enabling them to be more flexible, faster, and financially benefiting from cheap operating, maintenance, and service costs [1]. The cloud distributes storage and processing among servers and edge devices that provide self-services, enabling end users and stakeholders to receive ubiquitous and timely responses [2].

The cloud infrastructure is divided into three categories: private, public, and hybrid services, depending on the service

The associate editor coordinating the review of this manuscript and approving it for publication was Nitin Gupta.

being provided and the requirements of the customers [3]. The remote cloud configuration is for an organization hosting data within its own data center, where the organization is responsible for managing all cloud resources owned [4]. Since that infrastructure owns its private resources with limited organization-owned transactions, it provides enhanced security compared to public and hybrid cloud infrastructures. Albeit using a private cloud solution offers organizations better Security and control over their servers, it does necessitate a considerably higher level of IT experience than utilizing a public cloud. The public cloud setup is available to all externally registered companies over the internet, with the option to use the resources on a pay-per-use basis [5]. Given the shared communication channel, the public cloud is less secure but less expensive than the private cloud arrangement. The cloud infrastructure is controlled and maintained by a large Cloud Service Provider (CSP), responsible for establishing and encouraging the general public cloud and its IT resources. The hybrid cloud concept arose from the blurred distinctions between traditional private and public clouds, defined by location, ownership, and organizational requirements [5]. The hybrid cloud configuration combines the benefits of private and public clouds. The environment shares critical and non-critical information with the private and public infrastructure to ensure the appropriate Security while cutting resource management expertise and equipment costs [6].

These clouds empower their customers with infrastructure as a service (Iaas), platform as a service (Paas), and software as a service (SaaS) services that are hosted by outside providers and allowed access to consumers online [7]. The IaaS provides computing, networking, and data storage capabilities; PaaS offers a programming environment for users to develop code and run applications; and SaaS enables customers to run software that demands high processing over distant servers [8]. Besides the organization's distinctive requirements, the standard assessment metrics of cloud infrastructure are Security, cost, flexibility, service latency, responsiveness, encryption and decryption times, convergence speed, control over infrastructures, and complexity [9].

The healthcare sector is currently facing various financial challenges, such as managing multiple stakeholders for service delivery and an older population; nevertheless, medical informatics organizations may appreciate the benefits of the cloud paradigm for transmitting data and applications [10]. Cloud computing has the potential to address these challenges because medical data administration and analysis are expensive, and there are few appropriate software solutions [11]; consequently, cloud-based applications can bring solutions to the current problems confronting the healthcare sector [12]. However, even with the anticipated improvements, the rate of acceptance and efficient application of cloud computing within the healthcare industry still needs to improve. For instance, the retail industry has a 57% adoption rate of cloud computing, but the healthcare sector has a 31% adoption rate [13].

Security is one of the most significant barriers to adopting cloud computing within the healthcare system, influencing data integration, interoperability, real-time patient monitoring, and decision-making sharing among different healthcare physicians [14]. The cloud provides real-time patient monitoring, and clinicians frequently send sensitive health monitoring and classified medical data back and forth to cloud service providers resulting in a convoluted and insecure system that leads to a trade-off between computing complexity and security [15]. In this work, we presented a novel multi-objective-based healthcare data transmission in the cloud environment based on the BFL-PSO algorithm to meet the security requirements and solve the trade-off problem. The main three-fold contribution of this work is listed below.

- We investigated the data sanitization and restoration process to generate the keys and devised a multi-objective function for the hiding ratio, degree of modification, and information preservation ratio in conjunction with an optimization algorithm to determine the optimal key for patient's real-time monitoring and doctor's interchange of sensitive medical data back and forth to the cloud system.
- We addressed the multi-objective function by employing the Bee-Foraging Learning-based Particle Swarm Optimization (BFL-PSO) algorithm, which learns the hiding ratio, degree of modification, and information preservation ratio for the acquisition of the optimal key that ensures high Security for the transferring the healthcare data into the cloud system.
- We evaluated the suggested BFL-PSO algorithm against the cutting-edge Euclidean L3P-based Multi-Objective Successive Approximation (EMSA) [16], Shark Smell Optimization (J-SSO) [17], Improved Multi-Objective Particle Swarm Optimization (IMPSO) [18]. Hashed Needham Schroeder (HNS) Cost Optimized Deep Machine Learning (HNS-CODML) [19] security algorithms in terms of Security, delay time, encryption time, error rate, and convergence speed utilizing the Uniform Hospital Discharge Data set (UHDDS) [20] dataset.

The remainder of the work is organized as follows: Section II assesses the relevant results, and their benefits and drawbacks are enumerated. The system model of the proposed bee-foraging learning-based particle swarm optimization algorithm is demonstrated in Section III. the proposed BFL-PSO approach for the secured healthcare data in the cloud environment, as well as the multi-objective parameters, are discussed in Section IV. The findings and comparison study are discussed in Section V, and finally, Section VI concludes the work.

II. LITERATURE SURVEY

A Euclidean L3P-based Multi-Objective Successive Approximation (EMSA) algorithm is proposed by Sathya et al. [15] to conserve eHealth data, including the classification of health information into private and public categories. They encrypted sensitive information with an encryption key and retained the significant source of the encrypted keys. They assessed the proposed EMSA using the usefulness, fitness, and privacy parameters. Their findings revealed improved privacy for relatively large datasets, but they didn't consider the avoidance of all potential assaults.

Ahamad et al. [16] developed a Jaya-based Shark Smell Optimization (J-SSO) algorithm for the cloud sector, utilizing a two-step data restoration and sanitization approach to achieve optimal results. The parameters acquired from the optimum key are employed to verify health data security. The suggested model exhibited its potential to solve problems quickly and yield significant results; nevertheless, a sluggish convergence rate with low accuracy was observed. Consequently, an optimum output with a high convergence rate and accuracy have yet to be developed.

Devaraj et al. [17] have described the Firefly (FF) algorithm and the Improved Multi-Objective Particle Swarm Optimization (IMPSO) technique to reduce the search space for improving the acquisition of the optimum key. The search space is optimized, and the global best solution is chosen by locating a point and computing the distance to the optimal solution. The response time and resource usage are increased to facilitate effective selection, which results in data duplication.

Alzubi et al. [18] proposed the Hashed Needham Schroeder (HNS) Cost Optimized Deep Machine Learning (HNS-CODML) approach for secure data transmission. Their work derives the number of transitions and states from the classical Finite State Automata network model and employs Finite State Automata (FSA). The execution time, communication overhead, and cost estimate the model's effectiveness; however, security measures are not considered.

Rani et al. [20] adopted Hybrid Teaching and Learning Based Optimization (HTLBO) to solve encryption key optimization problems. The block cipher recognizes healthcare data encrypted by the network's IoT sensors. The number of users generates ciphertext data utilizing the Chinese Remainder Theorem (CRT), and the privacy and accuracy optimization is strengthened for the number of communicating users; moreover, the practical application of the work still needs to be addressed.

A Preferred Reporting Item for Systematic Reviews and Meta-analyses (PRISMA) technique has been proposed by Shukla et al. [21] to lower the latency of cloud and IoT. They exploited fog computing to reduce packet errors and identify the best path for the packets. They furthermore investigated the clustering mechanism to determine latency. As a result, their technique is highly efficient, albeit the emphasis was on latency rather than other security considerations.

Tamilarasi and Jawahar [22] introduced a novel hybrid lightweight encryption scheme employing a swarm optimization algorithm (HLE-SO). The lightweight features integrate HLE-SO with pallier encryption, which reduces the number of iterations required by the key space modifications algorithm. Furthermore, the approach encrypts the data and sends it to the end-user while considering encryption and decryption metrics while evaluating the suggested algorithm. As a result, the proposed method lowered error and processing time while boosting encryption time.

Anand et al. [23] have developed compression-then-encryption-based dual watermarking for healthcare to preserve Electronic Patient Records. The watermark is incorporated in the wavelet coefficient for data transmission in Electronic Patient Records. The redundant discrete wavelet transform (RDWT) covers the image, allowing it to be transferred effectively over the network. However, real-time implementation is challenging and results in significant complexity.

Mousavi and Ghaffari [24] present a novel Artificial Bee Colony (ABC) approach to secure irrigation systems by using Elliptic-Curve Cryptography (ECC) to generate private keys. The suggested study employs the D-dimensional space to determine the most suitable solution. Both the private and public keys are used to securely transmit data over the communication channel by storing the user's information. However, the mechanism for generating secure private keys needs to be researched, and therefore algorithms for private key generation are desired.

The cloud's Security can be gained by virtualized IP, data protection, controls, and policies; yet, it also has some shortcomings, such as data loss, loss of control and procedures, complexities, and more. To improve security in transmitting healthcare data in the cloud environment, resolving these problems is vital. Table 1 lists the limitations and benefits of prior works.

III. SYSTEM MODEL OF THE PROPOSED BEE-FORAGING LEARNING-BASED PARTICLE SWARM OPTIMIZATION ALGORITHM

Although cloud computing is a rapidly expanding technology, Security is one of the biggest worries since it must adhere to stringent security protocols for sensitive data like patient monitoring and hospital records. Therefore, the cloud system should ensure the safe transmission and receipt of sensitive data for patient monitoring and healthcare professionals. Moreover, the cloud grants access permission to a subset of users, reflecting a lack of data processing for all users in the cloud environment; to address the access permission issue, the cloud also supports the data sharing mechanism; nevertheless, this leads to the data breach problem. The cloud must establish a strong cyber security layer to ensure the cloud system's Security for both patient monitoring data and healthcare professional data. Therefore, the proposed work employs data sanitization and restoration techniques to construct secure keys for data transfer before utilizing the BFL-PSO to optimally determine the most suitable keys that enhance the security level for healthcare data, as shown in Fig. 1. The figure shows how healthcare data is encased using a two-step sanitization and restoration technique, with the former allowing the concealment of sensitive monitoring and other confidential data, preventing data breaches by

TABLE 1. A summary of the limitations of the previous algorithms concerning the cloud security measure in the healthcare system.

Reference	Algorithm/methods	Performance metrics	Limitations
Sathya et al. [16]	Euclidean L3P-based Multi-Objective Successive Approximation (EMSA)	Privacy perseverance is high and can be used for the large datasets	Only a specified attack can be circumvented
Ahamad et al. [17]	Jaya-based Shark Smell Optimization (J-SSO) algorithm	Swiftly provide security to the data	Optimized output is yet to be obtained
Devaraj et al. [18]	firefly (FF) algorithm and the Improved Multi-Objective Particle Swarm Optimization (IMPSO)	Improved resource usage and response time	Need improvement in the duplication of data
Alzubi et al. [19]	Hashed Needham Schroeder (HNS) Cost Optimized Deep Machine Learning (HNS-CODML) method	Execution time, communication overhead, and cost estimation is low	Security of the data is very low
Rani et al. [20]	Hybrid Teaching and Learning Based Optimization (HTLBO) to solve optimization problems	Privacy and accuracy are high	Implementation of the work in the real-time applications show less accuracy
Shukla et al. [21]	Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) technique	Provides better accuracy	Not obtained the required latency
Tamilarasi et al. [22]	hybrid lightweight encryption using a swarm optimization algorithm (HLE–SO)	Reduced processing and error	Decryption time is higher
Anand et al. [23]	compression-then-Encryption-based dual watermarking for healthcare	Security is high	The real-time implementation is complicated and produces high complexity
Mousavi et al. [24]	Artificial Bee Colony (ABC) algorithm to secure irrigation systems. Elliptic-Curve Cryptography (ECC)	Security of the data is high	Generation of the private key is not at all secured, hence need a better algorithm

unauthorized users. Subsequently, it leverages the BFL-PSO algorithm to resolve the multi-objective function and learn the encased ratio, degree of modification, and information preservation ratio to acquire the optimal key that guarantees high Security for transmitting medical data into a cloud system. The latter mechanism then decrypts the data using optimally chosen keys for the authorized users, consequently heightening Security and processing through a two-step sanitization, restoration, and optimization algorithm.

IV. PROPOSED BFL-PSO APPROACH FOR THE SECURED HEALTHCARE DATA IN THE CLOUD ENVIRONMENT

This section delves into the mechanism of the proposed multi-objective function for the cloud-based healthcare system, which employs data sanitization, restoration, and the BFL-PSO algorithms to encapsulate data, pick optimal keys, and restore data for authorized users.

A. THE UNIFORM HOSPITAL DISCHARGE DATASET

The Uniform Hospital Discharge Dataset (UHDDS) [25] was utilized to investigate the cloud environment's security through the sanitization and restoration process for the data-encased and restoration processes, as well as for optimum key selection using the suggested BFL-PSO algorithm. The UHDDS was a project of the Department of Health, Education, and Welfare, the forerunner of today's Department of Health and Human Services (HHS), and it offered patients access to their treatment data, including information on their Medicare and Medicaid coverage. Additionally, it provides sensitive information regarding the inpatient's symptoms and

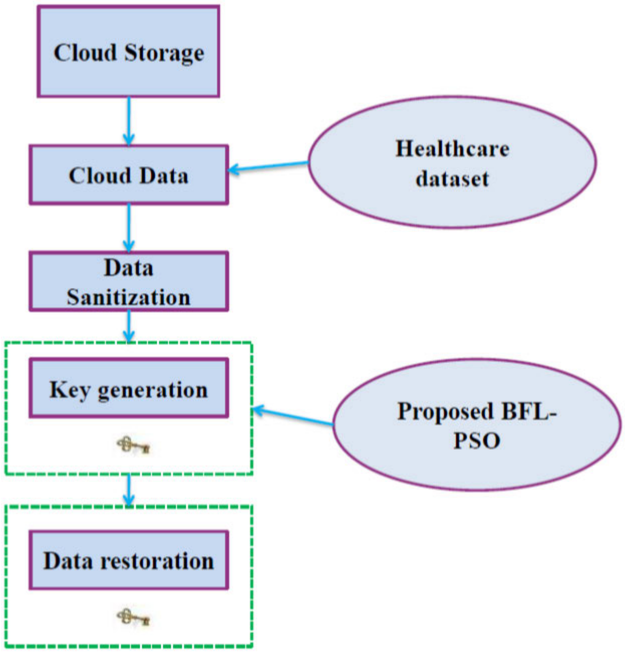


FIGURE 1. Illustration of the system model of the proposed BFL-PSO approach for enhancing Security in cloud systems for healthcare data.

reports on the primary treatment procedure, both before and after the diagnosis.

B. THE SANITIZATION AND RESTORATION MECHANISMS FOR DATA ENCASING AND RESTORING

The generation of a key matrix commences with binary data conversion in the cloud system, followed by the XOR operation to sanitize [26] the binary data that was transformed from the healthcare dataset, as depicted in the schematic diagram in Fig. 2. Meanwhile, the suggested BFL-PSO selects the best key among the generated keys, ensuring high Security and preventing unauthorized users from accessing the sanitized data. Next, the generated key and the cloud data are converted into binary form, and its total binary number is converted into decimal form for further processing. Following that, Eq. (1) is used to perform the XOR operation, which leads to the generation of sanitized data from the original data in addition to the generated key matrix data. This mechanism conceals sensitive data, enhancing the Security of the cloud system and offering data protection. The same XOR process is employed in the data restoration mechanism for permitted access, which utilizes the duplicate keys on the encrypted data to reinstate the encapsulated sensitive data, as shown in Eq. (2).

$$Fs' = Fs \oplus K2 \tag{1}$$

$$F\tilde{s} = Fs' \oplus K2 \tag{2}$$

The original data from the cloud is denoted as Fs, and after sanitization, the data is represented Fs', with the key generated after the optimization process labeled as K2. Likewise, the restored data is indicated as $F\tilde{s}$ at the restoration end.

C. THE KEY GENERATION MECHANISM

Once the pool of keys has been generated using the sanitization as mentioned above and the restoration mechanism, the suggested BFL-PSO algorithm is employed to determine an optimal key that ensures the highest level of Security. The key generation process entails the transformation into a new framework utilizing the Kronecker technique. Following that, the Kth key converts to the $K1$ matrix with a size of $\sqrt{W} \times R_{max}$, for instance, when the Kth key size is $K = \{6, 8, 1\}$ the resultant $K1$ matrix can be retrieved as shown in Eq. (3).

$$K1 = \begin{bmatrix} 6 & 6 & 6 \\ 8 & 8 & 8 \\ 1 & 1 & 1 \end{bmatrix}_{\sqrt{W} \times R_{max}} \tag{3}$$

The total number of records transacted is represented by W, which results in key duplication, as demonstrated by the rows in Eq. (3), necessitating a mechanism for determining the optimal keys. To derive the optimal key denoted by $K2$ from a population of keys with duplication, we utilize the BFL-PSO algorithm, as detailed in the subsequent section.

Lemma 1: If $(K_r)_{r=1}^{\infty}$ is an infinite series of real integers that conforms to $\sum_{w=1}^{\infty} K_w = s$ If something exists and is limited, then we have all got to $0 < b_1 \leq b_2 \leq b_3 \leq \ldots..\ and\ b_r \to \infty$ that

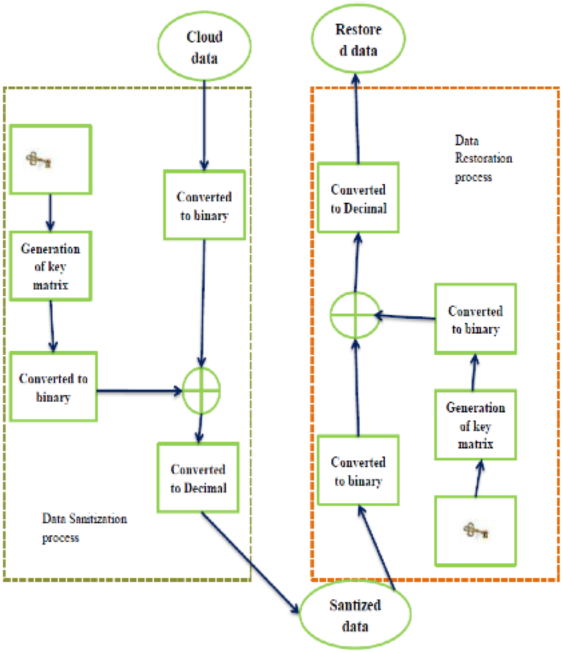


FIGURE 2. The data conversion and the sanitization and restoration processes for the generation of keys and optimal key selection through the proposed BFL-PSO approach.

$$\lim_{r\to\infty} \frac{1}{b_n} \sum_{n=1}^{r} b_n K_w = 0$$

Proof: Let L_n indicate the important partial amounts. Summarizing using components

$$\lim_{r\to\infty} \frac{1}{b_n} \sum_{n=1}^{r} b_n K_w = L_K - \lim_{r\to\infty} \frac{1}{b_n} \sum_{n=1}^{r} (b_{n+1} - b_n) L_n$$

Select any $\varepsilon > 0$. Select N now so that itL_n is near s for k > N. This can be done as the series $L_n$approaches s. The right half is then:

$$L_K - \frac{1}{b_k} \sum_{n=1}^{N-1} (b_{n+1} - b_n) L_n - \frac{1}{b_k} \sum_{n=N}^{k-1} (b_{n+1} - b_k) L_n$$
$$= L_K - \frac{1}{b_k} \sum_{n=1}^{N-1} (b_{n+1} - b_n) L_n$$
$$- \frac{b_k - b_N}{b_k} s - \frac{1}{b_k} \sum_{n=N}^{k-1} (b_{n+1} - b_k)(L_n - s)$$

Let n now extend to infinite. s receives the first term, and the third term wipes it out. The second component equals "0" (as the sum is a fixed value). The final component is limited by $\in (b_k - b_N)/b_k \leq \in$ because the b sequence is growing.

D. THE BEE-FORAGING LEARNING (BFL) MODEL

Since the suggested optimization algorithm is based on the bee-foraging learning model, we investigate it by employing the ABC division-of-labor approaches outlined in [27]. The model is composed of three main stages: employed learning, onlooker learning, and scout learning with the personal location designated by P_b, velocity V_i, and own location L_i portrayed through the particle N initialization procedure.

1) EMPLOYED LEARNING

The employed learning level demonstrates the behavior of particle swarm optimization as employee bees in the ABC algorithm, with the location and velocities of each particle updated depending on the Learning of personal and global ideal locations denoted by P_b and G_b, respectively. The following Eq. (4) is used to accomplish the modifications.

$$\begin{cases} V_i^{new} = & l\left(V_i^{old}, L_i^{old}, P_{bi}, G_b\right) \\ L_i^{new} = & L_i^{old} + V_i^{new} \end{cases} \tag{4}$$

where the variables L_i^{old} and V_i^{old} represent the location and velocity of the previous iteration, and the variables L_i^{new} and V_i^{new} are the updated or new location, and the velocity, with l being the upgrading velocity factor that replaces the local location L_i^{new}, instead of the global location G_b. Moreover, the remaining particles are updated by incrementing the counter variable as $CN(i) = CN(i) + 1$, which leads to the best position and the reset operation denoted with $CN(i) = 0$.

2) LEARNING OF ONLOOKER

Taking into account the onlooker bees mentioned in ABC [28], the particle with the best fitness values is sought in this onlooker stage; consequently, the best fitness value of each particle F_{b_i} is determined employing Eq. (5) and the probability of the i^{th} particle P_i being chosen can be computed according to Eq. (6).

$$Fit(L_i) = \begin{cases} \frac{1}{1+F_{b_i}} & F_{b_i} \geq 0 \\ 1 + |F_{b_i}| & otherwise \end{cases} \tag{5}$$

$$P_i = \frac{Fit(L_i)}{\sum_{i=1}^{M} Fit(L_i)} \tag{6}$$

The roulette technique identifies particles based on P_i values so that the particle with the largest value with the highest P_b value is regarded as the optimal value. For instance, considering the j^{th} chosen particle, the new location L_j^{new} based on the P_b value can be estimated and then compared to the same value; if the value is higher than the P_b, the estimated L_j^{new} value is substituted. Then, again, the remaining particles are updated by incrementing the j^{th} counter variable as $CN(j) = CN(j)+1$ that leads to the best position and the reset operation denoted with $CN(j) = 0$.

3) SCOUT LEARNING

The scout learning stage recognizes particles that fail to update their P_b value as exhausted until a certain number of iterations, with the positions, velocity, and P_b values becoming randomly re-initialized when the particles are evicted from the search space.

E. THE PROPOSED BEE-FORAGING LEARNING ENABLED PARTICLE SWARM OPTIMIZATION ALGORITHM

The BFL-PSO technique may be used to tackle various optimization problems by optimizing system parameters using the BFL model as a foundation. Therefore, the proposed BFL-PSO algorithm employs the BFL model in conjunction with the concept of biogeography-based Learning PSO to upgrade the velocity and location through generated Eq. (7).

$$\begin{cases} V_i^{new} = & \lambda \times A.random\left(P_{b_{\varepsilon_i}} - l_i^{old}\right) \\ L_i^{new} = & L_i^{old} + V_i^{new} \end{cases} \tag{7}$$

The inertia weight λ and learning factor A are crucial variables in the particle swarm optimization process. The inertia weight regulates the behavior of the particles in the swarm, enabling them to explore more of the search area. In contrast, the learning factor regulates the rate at which the particles update their velocities and locations, enabling them to converge on a solution swiftly. The optimization method may be modified to find better solutions in less time by modifying the values of these parameters. In this instance, λ is the inertia weight supplied in the range [0, 1], and A is the learning factor, a uniformly distributed random vector for values in the [0, 1] range. Finally, the total of all the particles' personal best placements is found, which is represented by $P_{b_{\varepsilon_i}}$. Figure 3 depicts the algorithm flowchart of the proposed BPLF-PSO, performing the following main steps.

1) ***Initialization:*** Initialize the particles' positions, velocities V_i and personal best p_{best} placements L_i with random values. Estimate the particles using Eq. (5) and store the G_{best} position. While the criteria are not met, Apply employed Learning.
2) ***Movement:*** Move the particles according to the velocity vector and update the personal best placements using Eq. (7).
3) ***Evaluation:*** Evaluate the fitness of the current positions and compare them with the personal best placements. If the new position is better than the old placements, then $p_{best} = L_i^{new}$ otherwise, the remaining particles are updated with incremental the counter variable as $CN(i) = CN(i)+1$ that lead to the best position and the reset operation denoted with $CN(i) = 0$.
4) ***Replacement:*** Replace the personal best placements with the better fitness value using the Learning of onlooker from Eq. (5) and Eq. (6) and continue the process similar from the previous steps till the optimal solution. Consequently, the Learning of scout is estimated and updated to the best solution.
5) ***total:*** Calculate the total of all the particle's personal best placements from employed, onlooker, and scout learning of all stages.
6) ***Termination:*** Terminate the algorithm if the total of all the particles' personal best placements is equal to $P_{b_{\varepsilon_i}}$.

Lemma 2: The finest particle will eventually arrive at location G_b.

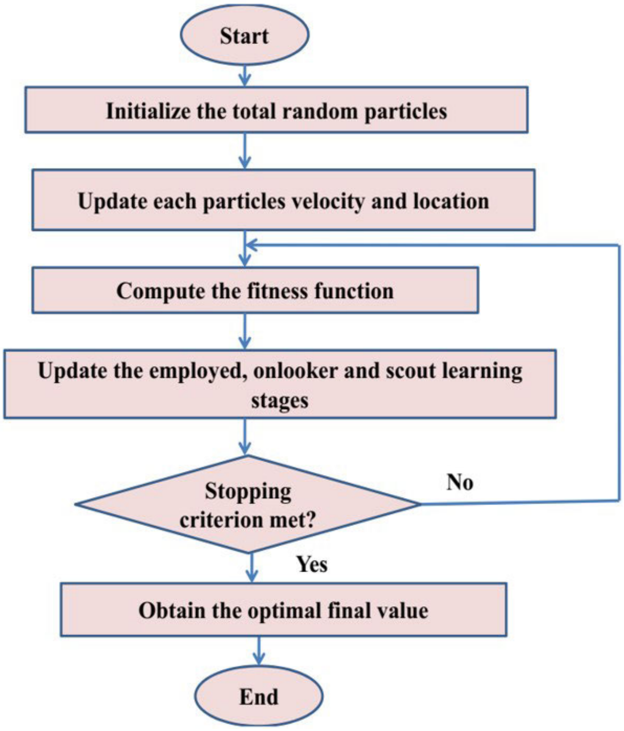

Start
Initialize the total random particles
Update each particles velocity and location
Compute the fitness function
Update the employed, onlooker and scout learning stages
Stopping criterion met?
No
Yes
Obtain the optimal final value
End

FIGURE 3. The flowchart of the proposed bee-foraging Learning enabled particle swarm optimization algorithm.

Proof: Let b serve as a representation of the particle's globally best score. After that, $G_{b_i} \triangleq G_b$. The trajectory of the particle is evaluated by the theory as,

$$\lim_{i\to+\infty} V_i = L_1 = \frac{\phi_1 G_b + \phi_1 G_b \epsilon_i}{\phi_1 + \phi_2} \tag{8}$$

This is true for each V_i coordinate, so that

$$\lim_{i\to+\infty} V_{b,i} = \frac{\phi_1 G_b + \phi_1 G_b \epsilon_i}{\phi_1 + \phi_2} = G_b \underset{i}{\epsilon} \tag{9}$$

This outcome is immediately applicable to the BFL-PSO's predictable variant. Furthermore, this result can be readily expanded to the stochastic case using Poli's most recent findings because $G_{b_i}{=}G_b\epsilon_i$. We will now include the other elements in this outcome.

F. MULTI-OBJECTIVE MODEL FOR OUR PROPOSED CYBER SECURITY-BASED CLOUD STORAGE FOR THE HEALTHCARE DATA

This section detailed the multi-objective function for the hiding ratio, degree of modification, and information preservation ratio using the BFL-PSO algorithm. Our proposed BFL-PSO algorithm fitness function optimizes the parameters of these four major objectives for the acquisition of the optimal key that ensures high Security for transferring the healthcare data into the cloud system.

1) HIDING RATION

The ratio of sensitive data to be concealed during the sanitization procedure [29] is determined by the hiding ratio, which is described by Eq. (10).

$$F_D = abs(F_1 - F_2) \tag{10}$$

The original data points F_1 and F_2 are utilized to compute the difference (distance) and is by the index F_D, where the non-zero F_D indices are denoted by M and can be computed using Eq (11).

$$H = \frac{M}{I_i} \tag{11}$$

where H is the hiding ratio, and the total number of data indexes is denoted as I_i, with better performance with a higher value of H and vice versa.

2) DEGREE OF MODIFICATION

The Euclidean distance between the original and sanitized data is used to calculate the degree of modification (Q), which is expressed as a percentage and computed using Eq. (12).

$$Q = Fs - F\tilde{s} \tag{12}$$

3) SOLUTION ENCODING

The generation of keys is contingent on the number of transactions or the size of the data, and the optimization of the generated key through the sanitization and restoration mechanism for the optimal key with an improved security level is accomplished by incorporating the BFL-PSO algorithm.

4) INFORMATION PRESERVATION RATIO

Information preservation indicates the fraction of non-sensitive data that is encapsulated throughout the sanitization process and is defined by the reciprocal value of the information loss, as stated in Eq. (13).

$$PI = \frac{M}{TP} \tag{13}$$

where TP is the total number of indexes that are preserved, where the higher value of PI results in stronger security measures and vice versa.

5) FINAL OBJECTIVE FUNCTION

The final objective function, Eq. (14), integrates the hiding ratio, degree of modification, and preservation ratio to yield an optimal key from the collection of generated keys.

$$FO = Q + (1 - H) + (1 - PI) \tag{14}$$

Here, Q denotes the degree of modification, H indicates the hiding ratio, and PI denotes the information preservation ratio.

V. EXPERIMENTAL ANALYSIS

In this section, we contrasted the multi-objective optimization-based encryption strategy with the diverse cutting-edge security approaches for improving the Security of cloud-linked smart healthcare data transmission.

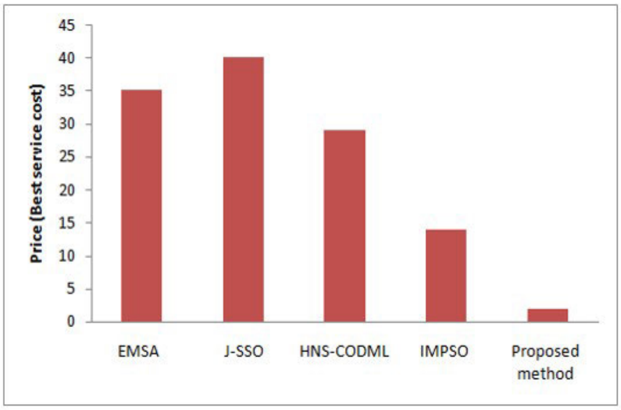


FIGURE 4. A comparison of the price or best service cost concerning the EMSA, J-SSO, HNS-COML, IMPSO, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

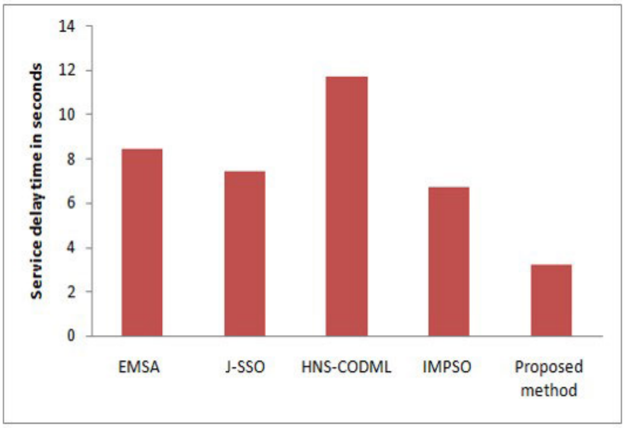


FIGURE 5. A comparison of the service delay time in seconds with EMSA, J-SSO, HNS-COML, IMPSO, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

A. PERFORMANCE ANALYSIS

Table 2 defines patient clinical information, and Table 3 provides several parametric descriptions based on health data size, in which parameters such as key size, keywords, number of rounds, and percentage of cipher security levels vary depending on health data size [30]. The suggested BFL-PSO-based security algorithm is assessed in terms of best price or cost and is shown in Fig. 4. The figure shows that the suggested algorithm outperforms the EMSA, J-SSO, HNS-CODML, and IMPSO approaches in terms of cost. Cost comparisons between the EMSA, J-SSO, HNS-CODML, IMPSO, and the suggested technique indicate costs of 35, 40, 29, 14, and 2 dollars, respectively. As a consequence, the proposed approach offers more cost-effective advantages when compared to the other security algorithms.

In Fig. 5, we show the Evaluation of service delay time to evaluate the suggested technique against the EMSA, J-SSO, HNS-CODML, and IMPSO approaches. According to the empirical investigation, the EMSA, J-SSO, HNS-CODML, IMPSO, and suggested approaches took 8.45 sec, 7.43 sec, 11.67 sec, 6.77 sec, and 3.2 sec, respectively.

The suggested approach, however, has a shorter service delay time than other current methods, such as EMSA, J-SSO, HNS-CODML, and IMPSO. We also took into account various situations, such as with and without optimization, and we recorded certain iterations to measure the response time, as shown in Fig. 6. The figure shows the response time for each security solution when 10, 20, 30, 40, and 50 iterations are considered, both with and without optimization. It is noticeable that the suggested BFL-based PSO algorithm achieves faster convergence than previous meta-heuristic models. Finally, the availability of BFL-based PSO optimization findings reduces execution time compared to the absence of optimization results [19]. Similarly, we analyzed the encryption times for the various techniques to assess the effectiveness of the proposed BFL-PSO algorithm and showed the findings in Fig. 7. The data bit size is essential in determining the encryption time since it consumes CPU cycles, which influences the encryption time. As a result, data bit sizes of 8, 18, 24, and 32 are selected for the encryption time evaluation. According to the figure, the suggested approach results in encryption times of 1, 5, 10, and 19 seconds for varied data volumes, which is significantly shorter than current methods such as EMSA, J-SSO, and HNS-CODML. Similarly, the performance in terms of decryption time for varied data sizes and results are shown in Fig. 8. The equivalent data bit sizes of 8, 18, 24, and 32 are used to evaluate the decryption time for each approach. We obtained decryption times of 1.5, 4.3, 9.9, and 18.78 seconds using the suggested approach for decrypting data of various sizes, and in comparison to current techniques such as EMSA, J-SSO, and HNS-CODML, the proposed strategy results in faster decryption.

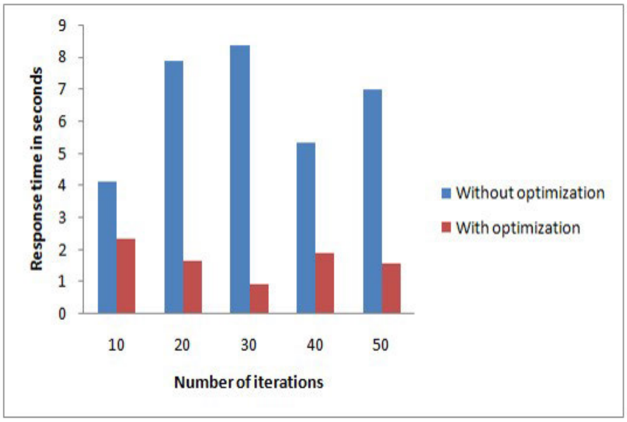


FIGURE 6. A comparison of the response time in seconds considering the proposed BFL-PSO algorithms for healthcare data in cloud system.

The suggested algorithm's convergence speed [31] with the number of iterations is also compared to the EMSA, J-SSOM, and HNS-CODML approaches. The findings are shown in Fig. 9 for the iterations of 10, 20, 30, 40, and 50 that were taken into consideration. In comparison to

TABLE 2. Clinical information of patients.

Patient data	Patient ID			
	C101	T202	S302	T121
Patient clinical parameter	Blood sugar	Body temperature	Heart rate	Blood sugar
Address details	Chicago	New Delhi	Atlanta	New Delhi
Doctor details	Subramanian	RockkBett	Subramanian	Scott

TABLE 3. Parameter description based on the size of health data.

Health data size	Key size	Keywords	Percentage of cipher security level	Number of rounds
8	16	2	60.78	16
16	20	1	60.45	20
24	24	2	63.23	20
32	30	1,2	655.34	24
40	16	2,3	63.84	24
48	20	2,3,4	65.34	20

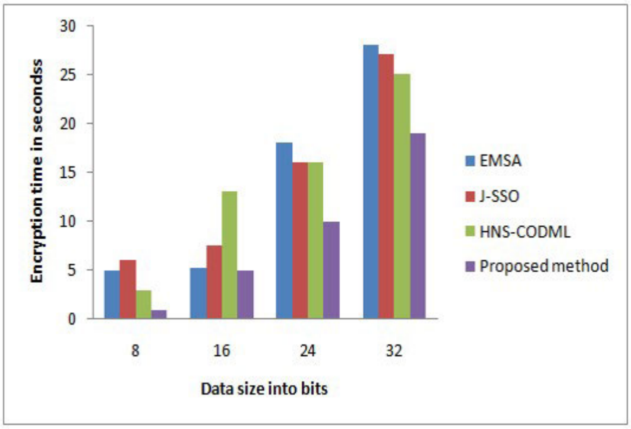


FIGURE 7. A comparison of the encryption time with varying data sizes according to the EMSA, J-SSO, HNS-COML, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

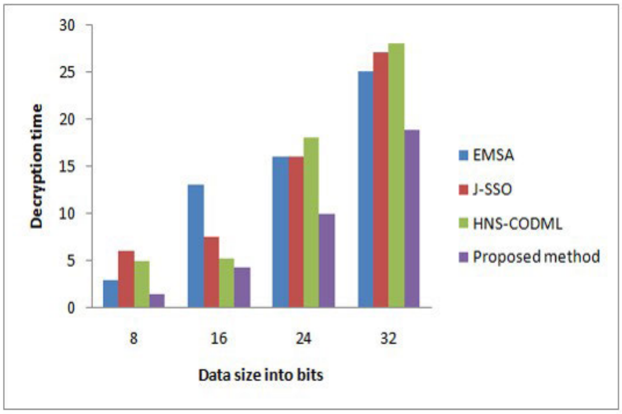


FIGURE 8. A comparison of the decryption time with varying data size according to the EMSA, J-SSO, HNS-COML, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

the cutting-edge security algorithms EMSA, J-SSOM, and HNS-CODML approaches, we have seen a faster convergence using the proposed algorithm. The suggested BFL state-of-the-art PSO's computational time [32] is contrasted to the EMSA, J-SSO, HNS-CODML, and IMPSO algorithms and the result is depicted in Figure 10. The figure demonstrates that the EMSA, J-SSO, HNS-CODML, IMPSO, and suggested approaches offer 12.38, 9.06, 10.34, 18.23, and 2.89 percentages of computational time, respectively. The figure shows that the proposed technique requires less computing time than the EMSA, J-SSO, HNS-CODML, and IMPSO algorithms.

Ultimately, we investigated error rate [33] measurement to analyze further the performance of the proposed BFL-PSO algorithm against the existing EMSA, J-SSO, HNS-CODML, and IMPSO approaches, and the results are shown in Fig. 11. The error rate values for the EMSA, J-SSO, HNS-CODML, IMPSO, and suggested techniques were 4.56, 7.34, 11.23, 3.23, and 1.02, respectively, shown in the figure. Compared to the EMSA, J-SSO, HNS-CODML, and IMPSO, the suggested BFL-PSO reduces the error rate by approximately 3.54, 6.32, 10.21, and 2.21, respectively.

B. DISCUSSION

The figure shows that the suggested algorithm outperforms the EMSA, J-SSO, HNSCODML, and IMPSO approaches in terms of cost, service delay time, response time, encryption times, decryption time, convergence speed, computational time, and error rate. In cost analysis, the J-SSO method has achieved 40 dollars, which is higher than the other methods. The IMPSO method has obtained 14 dollars, yet it is highly more than the proposed method because the developed model is highly cost-effective at 2 dollars. Moreover, the HNS-CODML method has taken a higher service delay time of 11.67 sec, which is 40% more than the other method and 70% higher than the proposed approach. However, the proposed method is 70% lesser service delay time than the earlier models. While increasing the size of the data, the encryption time will increase. However, the proposed method has achieved very less time as 1, 5, 10, and 19 seconds for data bit sizes of 8,18, 24, and 32. The earlier EMSA method has obtained higher encryption time for the 24th and 32nd data bits. The EMSA and J-SSO performance results are slightly identical. Consequently, the decryption time is also increased due to varying data bits. For small data bits, the

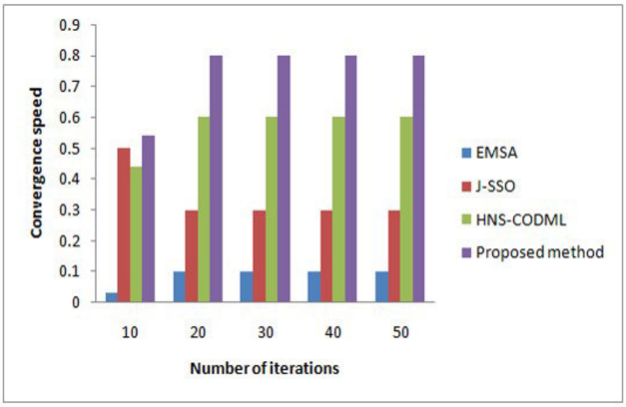


FIGURE 9. A comparison of the convergence speed with varying number of iterations following the EMSA, J-SSO, HNS-COML, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

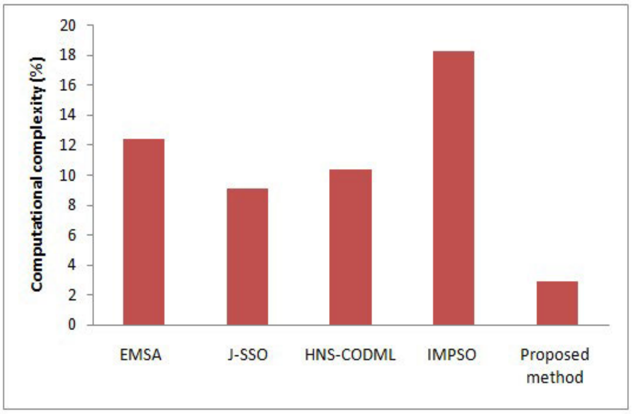


FIGURE 10. A comparison of the computational time concerning the EMSA, J-SSO, HNS-COML, IMPSO, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

conventional methods are performed faster, yet higher data bits consume more time for decryption. The proposed method takes less time and is 60% superior to the earlier methods. The convergence speed of the proposed method is 20% more than the HNS-CODML method and 50% and 70% more than the EMSA and J-SSO methods. Furthermore, the I MPSO computational complexity is higher than the earlier and proposed method, yet the proposed method has achieved very less complexity. The error rate of the HNS-COML method is more than the other methods. The analysis justified that the proposed method has achieved higher performance in terms of less cost, service delay time, encryption time, decryption time, computational time, error time, and higher convergence speed. The feasibility of the suggested approach in real-time applications is determined by various aspects, including the complexity of the problem, the amount of data, and the processing resources available. The suggested approach outperforms traditional approaches in terms of computing complexity, convergence speed, error rate, optimal encryption, and decryption durations, service and response times, and other factors. Besides, the suggested model also makes use of the PSO and bee foraging learning algorithms, which are well-known in optimization issues for their ease of use, adaptability, and capacity to manage several objectives concurrently. The fundamental PSO technique has undergone several extensions and modifications to meet a variety of optimization issues, including healthcare data security in cloud systems. Hence, it demonstrated a superior appropriateness for the realistic settings as compared to other options.

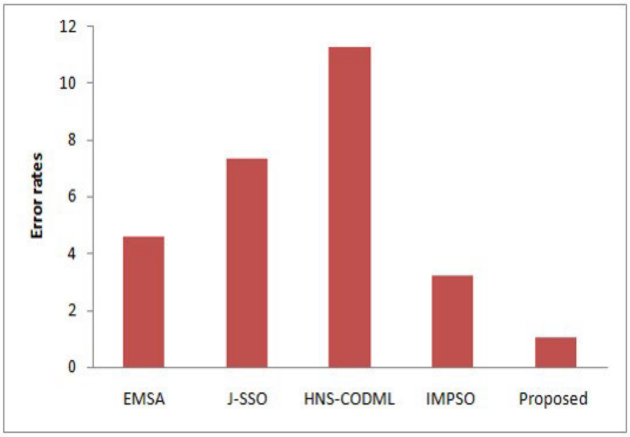


FIGURE 11. A comparison of the error rate with respect to the EMSA, J-SSO, HNS-COML, IMPSO, and the proposed BFL-PSO algorithms for healthcare data in cloud system.

VI. CONCLUSION

Cloud computing has the potential to facilitate the healthcare system by providing clinicians and other healthcare professionals with ubiquitous access to patient monitoring and other medical classified records for decision-making. Nonetheless, Security is one of the main obstacles that must be conquered to convince healthcare systems to adopt the cloud-based paradigm. In this study, we explored the data sanitization and restoration processes to generate the keys. We developed a multi-objective function for the degree of modification, hiding ratio, and information preservation ratio to enhance the Security of cloud-based systems for real-time patient monitoring and doctor-to-doctor exchange of sensitive medical data. The proposed model is highly effective for real-time practical application in validating real-time data. Consequently, by employing the Bee-Foraging Learning-based Particle Swarm Optimization algorithm, which learns the hiding ratio, degree of modification, and information preservation ratio to acquire the optimal key, high Security for transferring healthcare data into the cloud system is ensured. The proposed approach has achieved a 3.2 sec service delay time, 80% of convergence speed, 1 sec and 1.5-sec encryption and decryption time, and a 1.02% of error rate. The proposed BFL-PSO algorithm is evaluated against cutting-edge Euclidean L3P-based Multi-Objective Successive Approximation (EMSA), Shark Smell Optimization (J-SSO), Improved Multi-Objective Particle Swarm Optimization (IMPSO), and Hashed Needham Schroeder (HNS) Cost Optimized Deep Machine Learning (HNS-CODML) security algorithms in terms of Security, delay time, encryption time, error rate, and convergence speed. The results demonstrate that the proposed work effectively transfers healthcare data that is cleverly linked to the cloud environment while maintaining high-level Security. Future user identification during multi-level setup will use a secure authentication method, including artificial intelligence-based hashing in an authorization framework that can fend off fraud assaults and secure privacy.

ACKNOWLEDGMENT

The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work through the Research Groups Funding program Grant Code (NU/RG/SERC/11/4).

REFERENCES

[1] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of Things, big data, and cloud computing for healthcare 4.0," *J. Ind. Inf. Integr.*, vol. 18, Jun. 2020, Art. no. 100129.

[2] H. Wu, Z. Zhang, C. Guan, K. Wolter, and M. Xu, "Collaborate edge and cloud computing with distributed deep learning for smart city Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8099–8110, Sep. 2020.

[3] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.

[4] H. Ito, Y. Kinoshita, and H. Kiya, "A framework for transformation network training in coordination with semi-trusted cloud provider for privacy-preserving deep neural networks," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Dec. 2020, pp. 1420–1424.

[5] M. I. Malik, S. H. Wani, and A. Rashid, "Cloud computing-technologies," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 1–6, 2018.

[6] B. Wu, F. Tian, M. Zhang, H. Zeng, and Y. Zeng, "Cloud services with big data provide a solution for monitoring and tracking sustainable development goals," *Geogr. Sustainability*, vol. 1, no. 1, pp. 25–32, Mar. 2020.

[7] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, "CloudStrike: Chaos engineering for security and resiliency in cloud infrastructure," *IEEE Access*, vol. 8, pp. 123044–123060, 2020.

[8] F. Nadeem, "Evaluating and ranking cloud IaaS, PaaS and SaaS models based on functional and non-functional key performance indicators," *IEEE Access*, vol. 10, pp. 63245–63257, 2022.

[9] M. Zhu and H. Pham, "An empirical study of factor identification in smart health-monitoring wearable device," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 2, pp. 404–416, Apr. 2020.

[10] P. D. Kaur and I. Chana, "Cloud based intelligent system for delivering health care as a service," *Comput. Methods Programs Biomed.*, vol. 113, no. 1, pp. 346–359, Jan. 2014.

[11] H. S. G. Pussewalage and V. A. Oleshchuk, "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 1161–1173, Dec. 2016.

[12] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *J. Med. Internet Res.*, vol. 13, no. 3, Sep. 2011, Art. no. e1867.

[13] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *Int. J. Inf. Manage.*, vol. 43, pp. 146–158, Dec. 2018.

[14] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security challenges in healthcare cloud computing: A systematic," *Global J. health Sci.*, vol. 9, no. 3, pp. 157–168, 2017.

[15] A. Sathya and S. K. S. Raja, "Privacy preservation-based access control intelligence for cloud data storage in smart healthcare infrastructure," *Wireless Pers. Commun.*, vol. 118, no. 4, pp. 3595–3614, Jun. 2021.

[16] D. Ahamad, S. Alam Hameed, and M. Akhtar, "A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2343–2358, Jun. 2022.

[17] A. F. S. Devaraj, M. Elhoseny, S. Dhanasekaran, E. L. Lydia, and K. Shankar, "Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy efficient load balancing in cloud computing environments," *J. Parallel Distrib. Comput.*, vol. 142, pp. 36–45, Aug. 2020.

[18] J. A. Alzubi, R. Manikandan, O. A. Alzubi, I. Qiqieh, R. Rahim, D. Gupta, and A. Khanna, "Hashed needham schroeder industrial IoT based cost optimized deep secured data transmission in cloud," *Measurement*, vol. 150, Jan. 2020, Art. no. 107077.

[19] S. S. Rani, J. A. Alzubi, S. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmission on the Internet of Healthcare Things (IoHT) with lightweight block ciphers," *Multimedia Tools Appl.*, vol. 79, no. 47, pp. 35405–35424, 2020.

[20] S. Dara et al., "Machine learning in drug discovery: A review," *Artif. Intell. Rev.*, vol. 55, pp. 1947–1999, 2022, doi: 10.1007/s10462-021-10058-4.

[21] S. Shukla et al., "Improving latency in Internet-of-Things and cloud computing for real-time data transmission: A systematic literature review (SLR)," *Cluster Comput.*, vol. 26, pp. 2657–2680, 2023, doi: 10.1007/s10586-021-03279-3.

[22] K. Tamilarasi and A. Jawahar, "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm," *Wireless Pers. Commun.*, vol. 114, no. 3, pp. 1865–1886, Oct. 2020.

[23] A. Anand, A. K. Singh, Z. Lv, and G. Bhatnagar, "Compression-then-encryption-based secure watermarking technique for smart healthcare system," *IEEE Multimedia Mag.*, vol. 27, no. 4, pp. 133–143, Oct. 2020.

[24] S. K. Mousavi and A. Ghaffari, "Data cryptography in the Internet of Things using the artificial bee colony algorithm in a smart irrigation system," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102945.

[25] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 577–590, Jul./Aug. 2016.

[26] J. Liang, J. Ma, and X. Zhang, "Seismic data restoration via data-driven tight frame," *Geophysics*, vol. 79, no. 3, pp. V65–V74, May 2014.

[27] I. C. Trelea, "The particle swarm optimization algorithm: Convergence analysis and parameter selection," *Inf. Process. Lett.*, vol. 85, no. 6, pp. 317–325, 2003.

[28] X. Chen, H. Tianfield, and W. Du, "Bee-foraging learning particle swarm optimization," *Appl. Soft Comput.*, vol. 102, Apr. 2021, Art. no. 107134.

[29] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, nos. 3–4, pp. 313–336, 1996.

[30] M. Jia, Z. Yin, D. Li, Q. Guo, and X. Gu, "Toward improved offloading efficiency of data transmission in the IoT-cloud by leveraging secure truncating OFDM," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4252–4261, Jun. 2019.

[31] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Future Gener. Comput. Syst.*, vol. 82, pp. 375–387, May 2018.

[32] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, Nov. 2018.

[33] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: A systematic review," *Social Netw. Appl. Sci.*, vol. 2, no. 1, pp. 1–8, Jan. 2020.

REYAZUR RASHID IRSHAD received the B.Sc. degree from Aligarh Muslim University, Aligarh, India, in 2000, and the master's degree in computer application from Indira Gandhi University, New Delhi, India, in 2010. He is currently pursuing the Ph.D. degree with JJT University, Rajasthan. He is a Lecturer with the Department of Computer Science, Najran University, Saudi Arabia. He has published many articles in reputed journals and has attended some conferences. His research interest includes web-based applications.

SHAHAB SAQUIB SOHAIL received the bachelor's, master's, and Ph.D. degrees from Aligarh Muslim University computer as a major. He is interested in the area of social networks and privacy, recommender systems, personally identifiable information (PII), and users' online behavior. His primary work includes the design of a book recommender system for computer science graduates in India. He has also published more than 50 research articles with reputed publishers, such as Elsevier, IEEE, Springer Nature, Wiley, and Inderscience. He has also several patents on PII and user data privacy of social network sites.

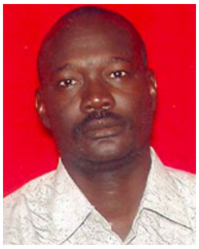
SHAHID HUSSAIN received the B.S. degree in mathematics and the M.Sc. degree in computer science from the University of Peshawar, in 2002 and 2005, respectively, and the M.S. and Ph.D. degrees in computer engineering from Jeonbuk National University, South Korea, in 2016 and 2020, respectively. He was a Postdoctoral Researcher with the Gwangju Institute of Science and Technology (GIST), South Korea, in 2020, and the University of Galway (UoG), Ireland, from 2020 to 2022. His research interests include smart grids, energy management, electric vehicles, smart grid infrastructure, optimization algorithms, micro-grid operations, distributed energy resources, peer-to-peer energy trading, and machine learning in medical applications (e.g. prediction and risk analysis of osteoporosis) using fuzzy logic, game theory, ontology, AI, and blockchain approaches and technologies. He achieved the Jeonbuk National University Presidential Award for academic excellence during the Ph.D. studies.

DAG ØIVIND MADSEN received the bachelor's degree from the University of Bergen, Norway, the M.Sc. degree from the London School of Economics, in 2002, and the Ph.D. degree from the Norwegian School of Economics, in 2011. He is currently a Professor with the University of South-Eastern Norway. His research interests include Industry 4.0/5.0 and applications of new technologies, such as big data and artificial intelligence in businesses and organizations.

MOHAMMED ALTAF AHMED was born in India. He received the bachelor's degree in engineering (electronics and communications), the master's degree in engineering and technology with a specialization in embedded systems, and the Ph.D. degree in electronics and communication engineering from GITAM University, Vishakhapatnam, India, for the thesis entitled "Design of Built-in Self-Test Controller using March Algorithm for Fault Diagnosis in Embedded Memories," in 2018. He has been a Senior Lecturer with the Quality and Development Unit, Computer Engineering Department, Prince Sattam bin Abdulaziz University, Saudi Arabia. He is currently focusing his research on VLSI and embedded systems, and nanomaterial and nano technologies. He has successfully implemented seven research grant projects in the same area and published research articles in leading academic journals.

AHMED ABDU ALATTAB received the B.Sc. degree in computer science from the University of Baghdad, Baghdad, Iraq, in 1997, the M.Sc. degree in computer science from the University of Technology, Baghdad, in 2002, and the Ph.D. degree in computer science-artificial intelligence from the University of Malaya, Kuala Lumpur, Malaysia, in 2013. He is currently an Assistant Professor with the Department of Computer Science, Najran University, Saudi Arabia. He is also an Assistant Professor with Thamar University, Yemen. He has published many papers in reputed journals and conferences. His research interests include artificial intelligence, image processing, image retrieval, image classification, object recognition, deep learning, natural language processing, computer vision, and neural networks.

OMAR ALI SALEH ALSAIARI received the B.Sc. degree in computer science from Tabuk University, Tabuk, Saudi Arabia, in 2008, and the M.Sc. degree in computer science from the University of New Brunswick, Fredericton, U.K., in 2013. He is currently a Lecturer with the Department of Computer Science, Najran University, Saudi Arabia. His research interests include artificial intelligence, software engineering, and data mining.



KHALID AHMED ABDALLAH NORAIN received the B.Sc. and M.Sc. degrees in computer science from the University of Khartoum, Sudan, Sudan, in 2000 and 2004, respectively. He is currently a Lecturer with the Department of Computer Science, Najran University, Saudi Arabia. His research interests include computer networks and software engineering.

ABDALLAH AHMED ALZUPAIR AHMED received the B.Sc. and M.Sc. degrees in computer science from the Sudan University of Science and Technology, Khartoum, Sudan, in 2004 and 2008, respectively. He is currently a Lecturer with the Department of Computer Science, Najran University, Saudi Arabia. He is also a Lecturer with the Sudan University of Science and Technology. His research interests include software engineering, data mining, healthcare, and geospatial analysis.