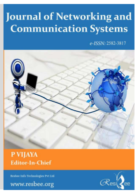
Vol.2 No.2 April 2019

Journal of Networking and Communication Systems

Received 7 December, Revised 13 February, Accepted 25 March



HDAPSO: Enhanced Privacy Preservation for Health Care Data

Jyothi Mandala
Department of CSE
GMRIT, Razam, Andhra Pradesh,India
jyothimandala780@gmail.com

Dr. M.V.P. Chandra SekharaRao
Department of CSE
RVR & JC College of Engineering
Guntur,Andhra Pradesh,India

Abstract: In the healthcare sector, information security and privacy are considered as a serious concern. All point towards the requirements for enhanced information protection, provider consolidation, the digital patient records, increased regulation, and the rising prerequisite for information between providers, patients, and payers are adopted. Almost all the conventional anonymization techniques are highly vigorous on data sanitization procedure but unfeasible for data restoration. However, recently some privacy preservation methods are developed, the accurateness of sanitization seems to be less. Therefore, this paper focused to evolve improved medical data preservation in healthcare data. Moreover, the proposed method highly relate to setting up an effectual sanitizing method for hiding the sensitive rules provided by clients. Hence, a secure key is produced that optimally chosen by exploiting Hybrid Dragonfly and Particle Swarm Optimization Algorithm (DAPSO) for sanitizing the medical data. Moreover, by the authorized user, the sanitized medical data is restored safely. In addition, the proposed technique is analyzed over existing techniques like Particle Swarm Optimization (PSO) and Dragonfly Algorithm (DA), and the results are achieved.

Keywords: Privacy preservation; Health care; Data anonymization; Data sanitization; Optimization algorithm

1.Introduction

Nowadays, health-clouds is broadly utilized in a lot of health applications like real-time health monitoring, insurance purpose, medical data analysis, and diagnosis of diseases, and so forth [1] [9]. In most instances, a suspicious third party will manage or retrieves the data whereabouts the original data owner [10] [11]. Therefore, the potential of diverse cloud security attacks is maximized [12]. In order to avoid these attacks, various access control mechanisms are identified. Despite the strong access control mechanism, there are numerous instances where a genuine user can deduce sensitive data namely SSN, name, and address, etc. Therefore, in the cloud databases, the inference control approaches should be applied to preserve the individuals' privacy [13] [14].

At present, in healthcare networks the "Electronic Medical Records" (EMRs) are well-known. It facilitates users to contribute their health data in a pliable as well as suitable manner [15] [16]. For instance, from a database the patient's doctor needs to retrieves the information in order to identify one's diagnostic report, preferably needs to search by various physical documents. At present EMR systems, to safely store and access EMRs, the health data is too perceptive, and it is a main confront [17] [18]. Since a huge number of EMRs is outsourced to the cloud, that does not have problems and exposed to probable intimidation as well as vulnerable to leakage loss, as well as theft. Before uploading them to the cloud a standard resolution is to present encryption to avoid EMRs from unauthorized access [19] [20].

Nowadays, numerous medical and health institutions have gathered a huge number of medical data, termed Electronic Health Records (EHRs) [21]. Moreover, these data are precious resources, which are exploited for medical decision making, prevention of disease, and a lot of other areas of healthcare [22]. In the health domain, several medical data further EHRs are also extensively exploited. For that reason, the data owner's tries to exploit the data collected to create profits by outsourcing or publishing the data to research organizations. On the other hand, the EHR data comprise sensitive information namely diagnosis and medication [23] [24]. Privacy can be breached if data subjects concerning sensitive information are revealed to others. Hence, by-laws numerous countries secure individuals' privacy in data publishing. These laws permit only the privacy preserved data for publication. Data anonymization is one of the most common exploits methods with a perspective of data privacy protection [31]. Nevertheless, other methods such as preventing data loss, tokenization of data, and so forth, are exploited for certain data privacy protection requirements. By faceting the personally identifying attributes, the privacy protection of data employing data anonymization is performed. Numerous optimization methods [27] [28] [29] [30] has been exploited for privacy preservation data.

© Resbee Info Technologies Pvt Ltd
https://doi.org/10.46253/jnacs.v2i2.a2

The main contribution of this paper is to enhance data preservation in healthcare data. The developed design highly concentrates on developing an effectual sanitizing technique. It is mainly developed for hiding the sensitive rules that are accessible by clients. Using the proposed HDAPSO method, a secure key is produced optimally for sanitizing the medical data. The remaining organization of the paper is as follows: Section 2 describes the literature review and section 3 defines the Objective model For Privacy Preservation and section 4 describes the proposed model. Section 5 summarizes the Proposed HDAPSO Algorithm for Optimal Key Generation. Section 6 describes the results and discussions and section 7 concludes the paper.

2. Literature Review

In 2018, WEI GUO et al [1] worked on Paradigm of Online Medical Prediagnosis (POMP) that use the logistic regression for the cloud environment to model privacy-preserving medical prediagnosis strategies. For users, it offers healthcare service without breaching their privacy. By using homomorphic encryption approaches, it was characterized to attain a privacy-preserving prediagnosis procedure against the encrypted data. In the diagnosing process, to minimize the computational cost, the presented POMP method embraces a Bloom filter and preprocessing approach. By experimental analysis, the proposed POMP method shows it can control several privacy threats and secure the privacy accomplishes.

In 2018, Xingguang Zhou et al. [2] presented two anonymous strategies they exploit to attain data confidentiality but also used to understand anonymity for individuals. Before attaining information from the EMR model, the first strategies attain modest protection, whereas the opponent selects attack targets. After interaction with the EMR system, the next strategies attain complete security, whereas adversaries adaptively select attack targets. Moreover, they offered exact proof demonstrating the security and anonymity of the presented strategies. In an anonymous model, a method that EMR owner could search for their EMRs was also presented. To speed up data processing the “online/offline” method was also applied for better user experience.

In 2019, Maoguo Gong and Ke Pan, Yu Xie [3] presented a novel model for a differentially private regression study on the basis of the significance. As stated in the magnitude of significance among the framework output and, the input features the proposed method changes the objective model in the polynomial form and troubles the polynomial coefficients. In particular, a smaller amount of noise to the coefficients was added for the polynomial indication of the objective model, which includes robustly appropriate features, as well as vice versa.

In 2019, Shouling Ji et al [4] worked on graph data anonymization, de-anonymizability quantification, and de-anonymization approaches. In the analysis, most anonymization strategies can partly or provisionally protect most graph value whereas losing some application value. However, the conventional anonymization strategies were susceptible to numerous or each and every rising structure-based de-anonymization attacks.

In 2017, Soohyung Kim and Yon Dohn Chung [5] proposed a new protocol for the privacy-preserving data gathering. On the contrary to conventional works, the proposed protocol won’t restrict the kind of anonymization technique as well as does not need the private channel. Also, the proposed method only needs the k-anonymity model, and therefore equal groups of data holders function as a method for privacy security. Furthermore, a greedy heuristic method was developed in order to deal with dynamic data holders and also discussed the probable attacks on the proposed protocol and avoidance of them.

In Mayank Kumar Kundalwal et al [6], presented a hybrid technique that involves two different inference control approaches such as k-anonymity and query set size restriction to guarantee the individuals’ privacy. To stop the sensitive data from inference attacks, a query set size restriction was exploited. However, k-anonymity was developed to secure the data between attacks. With satisfactory data use both these approaches achieve a certain privacy level. A rule set was also generated to maximize the privacy of healthcare data.

In 2018, Chun-Ta Li et al [7] Mohit et al, worked on a cloud-based health care system by a lightweight authentication protocol. They maintained their protocol assures flexibility of all renowned security attacks and presents numerous significant features namely patient anonymity and mutual authentication. Here, the authentication protocol has security flaws were also identified. Furthermore, an improved kind of their protocol was also introduced for cloud-assisted TMIS that be able to assure patient unlinkability and patient anonymity and avert the protection threats of report disclosure and report falsification attacks.

In 2018, Jiafeng Hua et al [8] presented a well-organized and primary medical diagnosis model for privacy-preserving. In this model, the accurate diagnosis methods were outsourced in an encrypted way to the cloud server, as well as users can access exact primary medical diagnosis service appropriately without revealing their medical data. In particular, unique rapid safe two-party vector supremacy strategies over ciphertext were proposed on the basis of the partial decryption and secure comparison approaches. Hence, the proposed method attains the user's query privacy preservation and the diagnosis outcomes and the privacy of diagnosis methods in the outsourced cloud server.

3. Objective model For Privacy Preservation

3.1 Objective Model

In eq. (1), F_O states the frequency of sensitive itemset in original data and F_S represents the frequency of sensitive itemset in sanitized data. Using eq. (1), (2) and (3), to produce the sensitive rules and association rules of the sanitized and original database, three objective functions c_1, c_2 and c_3 are calculated.

$$c_1 = \frac{F_S}{F_O} \tag{1}$$

$$c_2 = \frac{F_{NS}}{F_O} \tag{2}$$

In eq. (2), F_{NS} indicates the frequency of non-sensitive itemset in sanitized data. In eq. (3), the Euclidean distance among the sanitized data T' and original data T. In Eq. (4), c_4 indicates the distance among each item/element set of original and sanitized data. Additionally, the fitness function of the proposed approach is represented as F. Eq. (5) represents the objective model of the proposed privacy preservation in medical data.

$$c_3 = D\left(T, T'\right) \rightarrow \text{ Euclidean dis tan ce} \tag{3}$$

$$F = \frac{w_1 c_1}{\max\left[c_1, c_2\right]} + w_2\left(1 - \frac{c_2}{\max\left[c_1, c_2\right]}\right) + w_3\left(\frac{c_3}{\max\left(c_4\right)}\right) \tag{4}$$

$$G = \text{Min}\left(F\right) \tag{5}$$

3.2 System Model

Fig 1 shows the system model of privacy preservation. Here, the preservation of medical data includes that are data sanitization and data restoration. At first, the sensitive data undergo sanitization process, for hiding the sensitive data a key is produced. For producing the best key, a hybrid DAPSO method is used. Therefore, through the transmission line, the sanitized data in the database is transferred safely and in a while, it undergoes restoration procedure from that the sanitized medical data can be recovered economically by an authorized user.

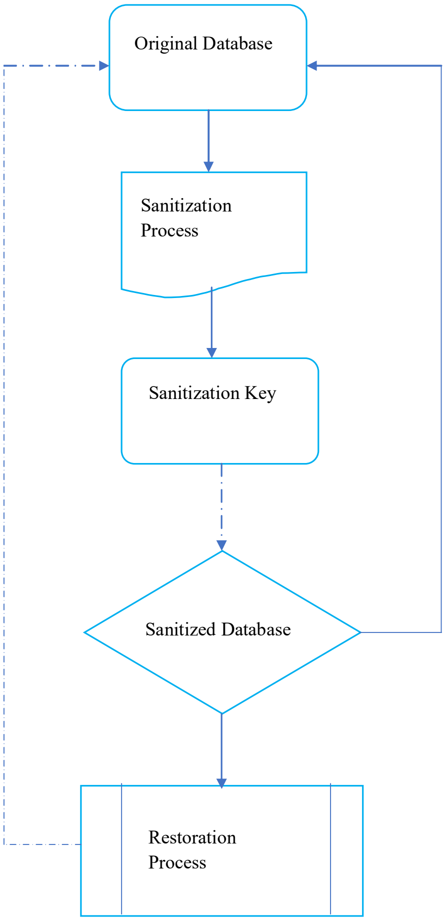


Fig. 1. *Systematic diagram of privacy preservation*

4.Proposed Model

Data sanitization: In Fig 2 shows the sanitization process. Here, T' is obtained from the sanitizing key, which generated from the original database by the key generation procedure. In order to perform the XOR function, the ensuing key matrix, T and X_2 is binarized. Eq. (6) states that later it is added up to the T' and unit step input is obtained.

$$T' = (X_2 \oplus T) + 1 \tag{6}$$

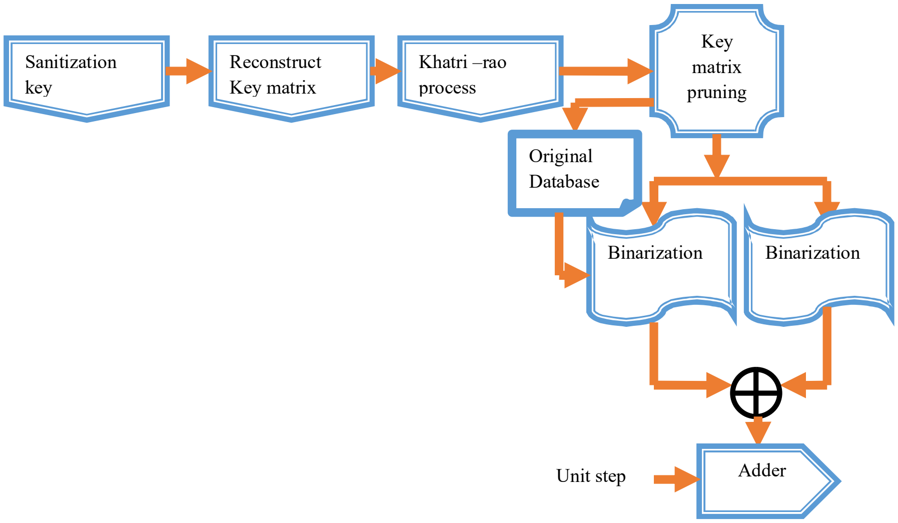


Fig. 2. *Diagrammatic representation of the sanitization process*
Fig. 3.

Key Generation:

Using the proposed HDAPSO method the key is created by initializing the population in an arbitrary manner for several keys that are pursued by the sanitization procedure from that the sanitized database is accomplished, and it is portrayed in Fig 3. Meanwhile, from the sanitization process, the sanitized database and original database attains an association rule and calculates objective functions, c_1, c_2 and c_3. Ultimately, updates the key-value continually until the maximum termination measure is obtained and creates the optimal-desired solution. By exploiting HDAPSO, a key is produced optimally for data sanitization process.

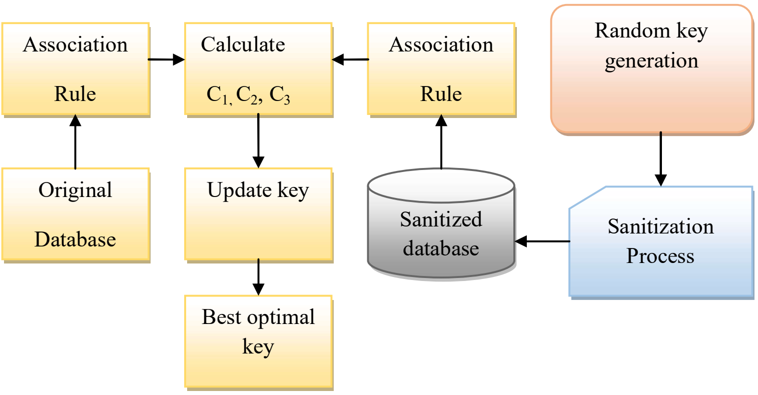


Fig. 4. *Architecture diagram of the key generation process*

Data Restoration: The decoding process is shown in Fig 4. X_2 obtained from key generation criterion need to binarized in the decoding process and T' obtained from sanitization block. From binarization block, the binarized database has been sanitized that is minimized from unit step input. Meanwhile, the database and binarized key matrix after reduction carry out XOR function after that restored database is recovered. Furthermore, it can also be stated as the sanitized key attained from the key generation procedure is used to reinstate the database T. It is used to generate the sanitized database T' whereas the lossless restoring can perform using eq. (6), in that X_2 states the sanitizing key matrix that is reconstructed from X and $\hat{T}$ indicates the restored data.

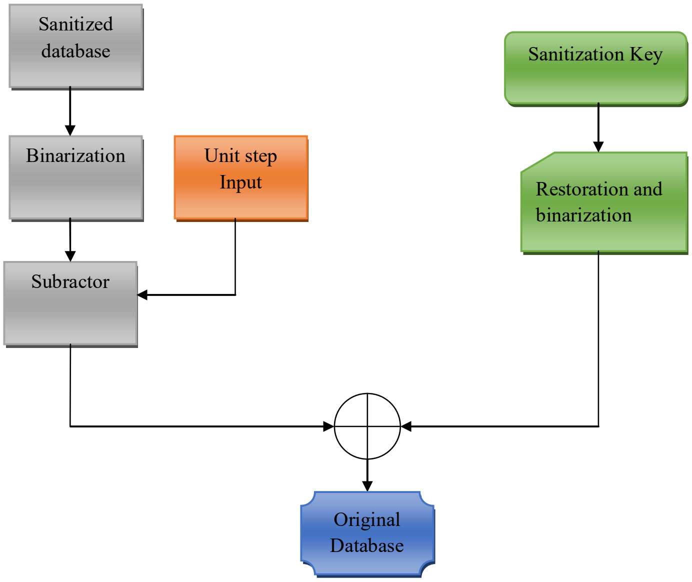


Fig. 5. *Schematic diagram of the decoding process*

5. Proposed HDAPSO Algorithm For Optimal Key Generation

5.1 Conventional Optimization Algorithms

Dragonfly Algorithm is a metaheuristic approach that is enthused by the dynamic as well as static swarming behaviors of dragonflies [25] in nature. The dragonflies need to achieve two aims, for instance, dynamic and static swarm. Numerous dragonflies swarm while roaming against different areas and long distances in the dynamic swarm that is the reason for the exploration phase. In a larger swarm, beside one direction and with local movements the dragonflies will move, as well as abrupt alters in the flying path that is in the static swarm that is appropriate for the exploitation phase.

By using five rules such as cohesion, attraction to an alignment, food source, separation, and disruption of an enemy the dragonflies' behavior can indicate. These five behaviors of dragonflies are explained and computed as stated below.

Eq. (7) used for the separation that is the evasion of the static deafening of individuals into other individuals in the neighborhood.

$$P_m = -\sum_{n=1}^{N} Z - Z_n \tag{7}$$

where N indicates the number of neighboring individuals, P_m indicates the separation of the m^{th} individual, location of the current individual is represented as Z the location of n^{th} the neighboring individual is represented as Z_n. Eq. (8) is used to calculate the position that indicates the velocity corresponding of individuals to the velocity of others in the neighbourhood.

$$B_m = \sum_{n=1}^{N} \frac{U_n}{N} \tag{8}$$

The position of the m^{th} individual represents as B_m, and U_n represents the velocity of n^{th} neighboring individual. Eq. (9) is exploited for the cohesion that represents the propensity of individuals to the center of mass of the neighbourhood.

$$H_m = \sum_{n=1}^{N} \frac{Z_n}{N} - Z \tag{9}$$

where H_m indicates the cohesion of the m^{th} individual. Eq. (10) is exploited to calculate the attraction towards a food source, which must be the main objective of any swarm to survive.

$$S_m = Z^{+} - Z \tag{10}$$

In eq. (10) Z^{+} represents the location of the food source and S_m indicates the food source of the m^{th} individual. Eq. (11) is exploited to calculate the distraction of an enemy that is an additional survival objective of the Swarm. Z represents the location of the food source and D_m indicates the position of an enemy of the m^{th} individual.

$$D_m = Z - Z^{+} \tag{11}$$

Step vector ΔZ and position vector Z are contemplated to imitate the artificial dragonflies' movement and update their positions. The direction of the movement of the artificial dragonflies was exploited by the step as well as it is indicated as eq (12).

$$\Delta Z^{t+1} = \left(pP_i + bB_i + hH_i + sS_i + dD_i\right) \tag{12}$$

where ΔZ^{t+1} indicates the step vector at iteration $t+1$, ΔZ^{t} indicates the step vector at iteration p, t, b, s, h and d are the alignment weight, separation weight, cohesion weight, enemy factor, and food factor respectively, and σ^{t} represents inertia weight factor at iteration and is computed by Equation (13).

$$\sigma^{t} = \sigma_{max} - \frac{\sigma_{max} - \sigma_{min}}{iter_{max}} \times iter \tag{13}$$

where σ_{max} set as 0.9 and σ_{min} set as 0.4, $iter_{max}$ indicates the maximum iteration and *iter* represents the iteration. Eq. (14) is exploited to update the position of the artificial dragonflies. Here, Z^{t} indicates the position at iteration t and Z^{t+1} represents the position at iteration $t+1$.

$$Z^{t+1} = Z^{t} + \Delta Z^{t+1} \tag{14}$$

The artificial dragonflies require to moves around the search space when the search space does not present a neighboring solution and random walk (i.e.,) Levy flight is applied to enhance their stochastic behavior. As a result, eq. (15) is used to compute the position of the dragonflies. In eq. (16), d indicates the dimension of the position vectors, using eq. (16) levy flight is also calculated.

$$Z^{t+1} = Z^{t} + \mathrm{levy}(d) \times Z^{t} \tag{15}$$

$$\mathrm{levy}(d) = 0.01 \times \frac{r_1 \times \eta}{|r_2|^{1/\beta}} \tag{16}$$

Eq. (17) is used to compute two uniform arbitrary values r_1 and r_2 in a range of (0, 1), where ß indicates the constant which is 1.5, $\Gamma(x) = (x \quad 1)!$.

$$\eta = \left(\frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta \quad -1}{2}\right)}} \right) \tag{17}$$

PSO: Eberhart and Kennedy [26] introduced the PSO optimization algorithm, which is a population-based stochastic global optimization approach. The PSO is inspired by the schooling of fishes in their food hunting or flocking behavior of birds. The population moves around a multidimensional search space whereas each particle indicates a possible solution in the PSO system. Here, each particle comprises the information of control variables and is related to a fitness value, which represents its performance in the fitness space. Each particle m consists of its position $Z_m = (z_{m,1}, z_{m,2} \ldots\ldots z_m, N_{var})$.

Where, $U_m = (u_{i,1,} u_{i,2,} \ldots\ldots u_i, N_{var})$, personal optimal experience $Z_{pbestm} = (z_{pbestm,1}, z_{pbestm,2} \ldots\ldots z_{pbestm}, N_{var})$ and a swarm have a global best experience $Z_{gbest} = (z_{gbest1}, z_{gbest2} \ldots\ldots z_{gbest}, N_{var})$, N_{var} indicates the number of control variables. Each particle moves in the direction of its own personal optimal location offered at each iteration hitherto and in the direction of the global optimal location attained hitherto by particles in the swarm. Using eq. (18) and (19) the particles are operated

$$\begin{aligned} U_m^{t+1} = \sigma^t \times U_m^t + H_1 \times \mathrm{rand}_1 \times \left(Z_{pbestm}^t - Z_m^t\right) \\ + H_2 \times \mathrm{rand}_2 \times \left(Z_{gbestm}^{t+1} - Z_m^t\right) \end{aligned} \tag{18}$$

$$Z_m^{t+!} = Z_m^t + U_m^{t+1} \tag{19}$$

where U_m^{t+1} represents the velocity of particle m at iteration $t+1$, U_m^t represents the velocity of particle m at iteration t, H_1 and H_2 are two positive acceleration constants, rand_1 and rand_2 are two uniform arbitrary values in a range of [0, 1], Z_m^t represents the location of particle m at iteration t, Z_{pbestm}^t represents the personal optimal location of particle m at iteration t, Z_{gbestm}^t represents the global optimal location between all particles at iteration t, and $Z_m^{t+!}$ is the location of particle m at iteration $t+1$.

5.2 Proposed HDAPSO Algorithm

To overcome the optimization problem numerous optimization methods have been proposed for being trapped in the local optima when the methods attempt to identify the optimal solution.

Here, a new hybrid method is proposed, which combines the well-known points of the PSO as well as DA methods that are the exploitation of PSO and the exploration of DA. Initially, in DA the global solution area of the dragonflies are initialized to discover the search space. Subsequently, the optimal location of DA is attained.

Then, the attained optimal position from DA is substituted as the global optimal position in the (eq.18)). Later, the PSO approach, exploiting the global optimal position from DA that is the exploitation phase, operates, permitting it to present the usual optimal solution. The eq. (18) and (19) indicates the location as well as velocity equations of PSO.

$$U_m^{t+1} = \sigma^t \times U_m^t + H_1 \times \mathrm{rand}_1 \times \left(Z_{pbestm}^t - Z_m^t\right) + H_2 \times \mathrm{rand}_2 \times \left(Z_{DA}^{t+1} - Z_m^t\right) \tag{20}$$

where Z_{DA}^{t+1} indicates the optimal position attained from DA at iteration $t+1$.

The application of the proposed HDAPSO technique for attaining the best key for protects restoration and sanitization of sensitive medical data can be defined as follows:

Algorithm: Pseudo code of the proposed method

```
Initialize the population of particles and dragonflies
For the initial population of dragonflies compute the objective functions
Find the nondominated solution and store them to primary archive
The food source is considered as the fitness value of the food source
Compute the parameters of DA $p, b, h, s$ and $d$
Enemy of DA and food source is updated
Eq. (12) is used to compute $P, B, H, S, D$
If a dragonfly has minimum one neighboring dragonfly, subsequently eq. (12) and (14) is used for step vector updation $\Delta Z$ and the location of dragonfly $Z_{DA}$ and if each dragonfly has no neighboring dragonfly, subsequently using eq. (15) update $Z_{DA}$ by Equation (15) and set $\Delta Z$ to be 0.
Subsequently $\Delta Z$ or $Z_{DA}$ of the population is stimulated into its maximum/minimum limit if any component of each population breaks its boundary.
Set the optimal location attained from DA as the global optimal of PSO $Z^{gbest}$
Using eq. (19) update the position of the particle as $Z_{PSO}$ and update the velocity of the particle $U$
Subsequently $U$ or $Z_{PSO}$ of that population is moved into its minimum/maximum limit if any component of each population breaks its limit.
Compute the objective functions of the newly generated population.
Using the Pareto front approach to store the nondominated solutions to the archive and then update the archive.
    If the maximum number of iterations is attained, the method is halted; else compute the parameters of DA $p, b, h, s$ and $d$
```

6. Results and Discussions

6.1 Experimental Procedure

The proposed HDAPSO approach for medical data preservation has experimented, and the outcomes were attained. The experimentations were performed exploiting four medical datasets, such as Autism-Adolescent dataset, Cryotherapy dataset, Autism-Child dataset, and Immunotherapy dataset. In addition, the outcomes were compared with existing approaches namely PSO, and DA on the basis of the recovery data.

6.2 Restoration Analysis

In Table 1-4, the restoration analysis of proposed HDAPSO method for four data is shown. In Table 1, the proposed method is 16% and 26% better than the conventional DA and PSO method for c_1. The fitness function of the proposed method is 13% and 21% better than the conventional DA and PSO. Table 2 demonstrates the restoration analysis of the Autism-Child-Dataset. Here, the proposed method is 10% and 12% superior to the conventional DA and PSO methods with respect to the c_3. The fitness function of the proposed method is 11% and 13% better than the conventional DA and PSO method.

Table 1. *Restoration Study of Autism-Adolescent-Dataset*

Methods	DA	PSO	Proposed
c_1	4.543106	5.124447	3.789728
c_2	1.857505	1.894766	0.928153
c_3	4.160502	3.219138	4.042105
F	2.197182	2.713697	1.348622

Table 2. *TRestoration study of Autism-Child-Dataset*

Methods	DA	PSO	Proposed
c_1	2.3426	2.57681	2.086145
c_2	1.841322	1.988125	0.767823
c_3	1.126236	2.475244	1.005355
F	2.822552	2.332345	1.462129

Table 3. *Restoration study of Cryotherapy-Dataset*

Methods	DA	PSO	Proposed
c_1	1.2785	1.2919	0.8976
c_2	2.4839	2.3245	1.9877
c_3	6.5674	8.2345	5.880
F	1.2945	1.3266	0.6976

Table 4.*Restoration study of Immunotherapy-Dataset*

Methods	DA	PSO	Proposed
c_1	1.2934	1.5234	1.0234
c_2	2.2245	2.7042	1.1126
c_3	1.2456	3.130	0.396
F	1.9456	1.44217	0.7101

In Table 3, the restoration analysis of cryotherapy dataset is demonstrated. Here, the analysis shows the proposed method is 21% better than DA and 25% better than PSO methods for c_2. Moreover, the fitness function of the proposed method is 17% better than conventional DA and 18% better than the conventional PSO method. Table 4 states that the restoration analysis of the immunotherapy dataset. For F, the proposed method is 31% and 33% better than the conventional DA and PSO methods. Here, the fitness function of the proposed method is 33% and 34% better than the conventional DA and PSO method.

7.Conclusion

In this paper, a privacy preservation method in healthcare data was presented. Primarily the proposed method concentrated on developing an effectual sanitizing method for hiding the sensitive rules offered by clients. A key was produced, which was optimally selected using the proposed HDAPSO approach for hiding the confidential medical data. In addition, by the authorized user, the sanitized data can safely improve. Then, the implemented method was classified with conventional methods, and the outcomes were obtained. The implemented scheme was analyzed on the basis of the analysis in terms of the several attacks for numerous approaches and enhanced results were achieved by the proposed method.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] W. Guo, J. Shao, R. Lu, Y. Liu and A. A. Ghorbani, "A Privacy-Preserving Online Medical Prediagnosis Scheme for Cloud Environment," IEEE Access, vol. 6, pp. 48946-48957, 2018.

[2] X. Zhou, J. Liu, Q. Wu and Z. Zhang, "Privacy Preservation for Outsourced Medical Data With Flexible Access Control," IEEE Access, vol. 6, pp. 14827-14841, 2018.

[3] Maoguo Gong, Ke Pan, Yu Xie, "Differential privacy preservation in regression analysis based on relevance" Knowledge-Based Systems, vol. 173, pp. 140-149, 1 June 2019.

[4] S. Ji, P. Mittal and R. Beyah, "Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1305-1326, Secondquarter 2017.

[5] Soohyung Kim, Yon Dohn Chung, "An anonymization protocol for continuous and dynamic privacy-preserving data collection", Future Generation Computer Systems, vol. 93, pp. 1065-1073, April 2019.

[6] Mayank Kumar Kundalwal, Kakali Chatterjee, Ashish Singh, "An improved privacy preservation technique in health-cloud", ICT Express, In press, corrected proof, Available online 30 October 2018.

[7] Chun-Ta Li, Dong-Her Shih, Chun-Cheng Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems", Computer Methods and Programs in Biomedicine, vol. 157, pp. 191-203, April 2018.

[8] Jiafeng Hua, Guozhen Shi, Hui Zhu, Fengwei Wang, Hao Li, "CAMPS: Efficient and privacy-preserving medical primary diagnosis over outsourced cloud",Information Sciences, In press, corrected proof, Available online 27 December 2018.

[9] Wang C , Ren K , Yu S , Urs KMR . Achieving usable and privacy-assured simi- larity search over outsourced cloud data. In: 2012 Proceedings IEEE INFOCOM, Orlando, FL; 2012. p. 451–9 .

[10] S. Kim and Y.D. Chung, "An anonymization protocol for continuous and dy- namic privacy-preserving data collection", Future Generation Computer Sys- tems, In press, corrected proof, Available online 8 September 2017.

[11] W. Newhauser, T. Jones, S. Swerdloff, W. Newhauser and R. Zhang, "Anonymization of DICOM electronic medical records for radiation therapy", vol. 53, pp. 134–140, 1 October 2014.

[12] A. Majeed, "Attribute-centric anonymization scheme for improving user pri- vacy and utility of publishing e-health data", Journal of King Saud University - Computer and Information Sciences, available online 31 March 2018.

[13] Wei R , Tian H , Shen H . Improving k-anonymity based privacy preservation for collaborative filtering. Comput Electr Eng 2018;67(April):509–19 .

[14] N M , Jiang X , Chen R , Fung BC , Ohno-Machado L . Privacy-preserving heteroge- neous health data sharing. J Am Med Inform Assoc 2013;20(3) .

[15] Yoo S , Kim S , Lee K-H , Jeong CW , Youn SW , Park KU , Moon SY , Hwang H . Electronically implemented clinical indicators based on a data warehouse in a tertiary hospital: its clinical benefit and effectiveness. Int J Med Inf 2014;83(7):507–16 .

[16] Gardner J , Xiong L , Xiao Y , Gao J , Post AR , Jiang X , Ohno-Machado L . SHARE: system design and case studies for statistical health information release. J Am Med Inform Assoc 2013;20(1):109 -16.

[17] Perera G , Holbrook A , Thabanea L , Fostera G , Willison DJ . Views on health in- formation sharing and privacy from primary care practices using electronic medical records. Int J Med Inf 2011;80(2):94–101 .

[18] Tamersoy A , Loukides G , Nergiz ME , Saygin Y , Malin B . Anonymization of longitudinal electronic medical records. IEEE Trans Inf Technol Biomed May 2012;16(May (3)):413–23 .

[19] Abouelmehdi K , Beni-Hssane A , KhaloufiH , Saadi M . Big data security and pri- vacy in healthcare: a Review. Procedia Comput Sci 2017;113:73–80 .

[20] Anjum A , Malik SuR , Choo K-KR , Khan A , Raza B . An efficient privacy mecha- nism for electronic health records. Comput Secur 2018;72(January):196–211 .

[21] Gkoulalas-Divanis A , Loukides G , Sun J . Publishing data from electronic health records while preserving privacy: a survey of algorithms. J Biomed Inf 2014;50:4–19 .

[22] Aggarwal CC , Yu PS . A general survey of privacy-preserving data mining mod- els and algorithms. Privacy-Preserving Data Mining 2008;34:11–52 .

[23] Demir S , Tugrul B . Privacy-preserving trend surface analysis on partitioned data. Knowl-Based Syst 2018;144(March):16–20 .

[24] Y. Wang, Z. Cai, Z. Chi, X. Tong and L. Li, "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems", vol. 129, pp. 28–34, 2018.

[25] Mirjalili, S. Dragonfly algorithm: A new meta-heuristic optimization technique for solving single-objective, discrete, and multi objective problems. Neural Comput. Appl. 2016, 27, 1053–1073. [CrossRef]

[26] Eberhart, R.; Kennedy, J. A New Optimizer Using Particle Swarm Theory. In Proceedings of the Sixth International Symposium on Micro Machine and Human Science (MHS'95), Nagoya, Japan, 4–6 October 1995; pp. 39–43.

[27] Archana H. Sable Haricharan Dhirbasi,Dr. Bondar Kirankumar Laxmanrao,"Application of Integral Transform to Recognition of Plastic Surgery Faces and the Surgery Types: an Approach with Volume based Scale Invariant Features and SVM",vol.6, no.3, pp.1061-1072, 2018.

[28] R Gupta Roy, D Baidya,"Speed Control of DC Motor Using Fuzzy-Based Intelligent Model Reference Adaptive Control Scheme",Advances in Communication, Devices and Networking, Lecture Notes in Electrical Engineering book series, Springer, vol. 462, pp.729-735, 2018.

[29] G Singh, VK Jain, A Singh, "Adaptive network architecture and firefly algorithm for biogas heating model aided by photovoltaic thermal greenhouse system", Energy & Environment, vol. 29 (7), pp.1073-1097, 2018.

[30] Vijayakumar Polepally, K Shahu Chatrapati,"DEGSA-VMM: Dragonfly-based exponential gravitational search algorithm to VMM strategy for load balancing in cloud computing";Kybernetes, vol.67, no.6;pp.1138-1157;2018.

[31] D. Menaga and Dr.S. Revathi,"Privacy Preserving using Bio Inspired Algorithms for Data Sanitization", International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC); pp. 201-206, 2018.