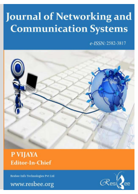
Vol. 2 No.4 Oct 2019

Journal of Networking and Communication Systems

Received 1 September, Revised 4 October, Accepted 31 October



Impact of Opposition Intensity on Improved Cuckoo Search Algorithm for Privacy Preservation of Data

G.K. Shailaja
Kakatiya Institute of Technology and Science
Warangal, Telangana, India
gujjarishailaja@gmail.com

Dr C.V. Guru Rao
S.R. Engineering College
Warangal, Telangana, India

Abstract: Nowadays, large amounts of data are stored and retrieved frequently in day-to-day life. The data stored in the system may contain sensitive data which necessitates the implementation of preserving privacy in big data. For this reason, Privacy-Preserving Data Mining (PPDM) models are emerged to handle the privacy problems by avoiding unauthorized access and misuse if sensitive data. In current years, a lot of researches were implemented to handle the preservation issues. However, the challenges due to large data and computationally expensive issues limit the performance of PPDM approaches. Thus, this paper plans to implement a new PPDM model with two stages such as data sanitization and data restoration. In both the sanitizing and restoring process, key extraction is a major process that is optimally selected by means of modified CSA approach called Opposition Intensity-based Cuckoo Search Algorithm (OI-CSA). Finally, the performance of the proposed model is analyzed by varying co to 0.2, 0.4, 0.6, 0.8 and 1, respectively.

Keywords: PPDM; Sanitization; Key Extraction; Restoration; OI-CSA; Hiding Failure

Nomenclature

Abbreviation	Description
PPDM	Privacy-Preserving Data Mining
OI-CSA	Opposition Intensity-based Cuckoo Search Algorithm
PPDP	Privacy Preserving Data Publishing
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
TPDM	Truthfulness and Privacy preservation in Data Markets
AAP-CSA	Adaptive Awareness Probability-based Crow Search Algorithm
LBSNs	Location-Based Social Networks

1. Introduction

In recent decades, with the advancement in technologies, large amounts of data are generated every day which are needed to be managed and utilized efficiently [7]. With the emergence of big data, handling a huge quantity of data becomes an easy task in daily life. Generally, the big data is deployed in many sectors such as medical sectors, government sectors, educational organizations and so on due to its efficiency and applications in handling and storing data. Typically, big data contains large, vague, structured and unstructured data, and particularly, it can have sensitive information about the user [6]. For instance, medical data of a patient may contain personal and health information of the patient. Similarly, governmental sector data contains data about its citizens which are highly sensitive which necessitated the introduction of privacy preservation to secure the sensitive data [9]. Classically, privacy preservation is a technique to attain access to high-quality data concerning preserving sensitive information of individuals in its raw form and protect data privacy [8].

Besides, the information fetched from diverse locations through internet/local profiles of the institutions is utilized by several sectors to make efficient decisions for applicant gratification [12]. This information is vulnerable to the attackers and hackers to hack the data which damages the reliability of the organization. For this reason, data privacy should be maintained while sharing information among third parties in order to protect the secrecy and reliability of the organization [11]. In addition to this, the raise in smart phone usage leads to the use of internet in terms of social media which contains all the

https://doi.org/10.46253/jnacs.v2i4.a4

personal details about an applicant. Furthermore, social media are highly vulnerable to attacks such as neighbourhood attacks, mutual friend's attacks, structural attacks, etc. All these cause necessities the innovation of privacy preservation techniques to keep secrecy and data integrity [15]. Traditionally, a lot of methods were introduced to handle privacy preservation issues in various fields. With the intension of eliminating the issues due to hackers, a novel and effective PPDP and PPDM were proposed in which PPDP deals with the differentiation of raw data for publishing and PPDM deals with the restriction of the quantity of data attained by the hacker [14].

Moreover, with the establishment of AI, ML techniques become popular and widely implemented in recent technologies. Besides, the DL techniques were introduced to handle supervised and unsupervised data [13]. For improving the ML and DL schemes, all such techniques are needed to be optimized by intelligence algorithms, evolutionary algorithms, and so on[10]. However, the limitations such as large data, data heterogeneity, and data vagueness bound the usage of metaheuristic algorithm. Moreover, Traditional models for data preservation are not sufficient to overwhelm the challenges and limitations in data mining which can be attacked from remote environments [13]. Thus in the field of privacy preservation, there is a large scope for future researches to preserve data in data streams more efficiently with intelligent approaches.

The organization of the paper is as follows: Literature review on data privacy preservation is presented in Section II. Section III represents the proposed data privacy preservation model such as data sanitization and restoration. Section IV discusses key encoding. Section V presents the results and discussions, and the paper concludes with Section VI.

2. Literature Review

2.1 Related Works

In 2019, Niu et al. [1] have proposed a data privacy preservation model using TPDM approach. Moreover, it was composed implicitly as an "Encrypt-then-Sign" format through partially homomorphic encryption with identity-oriented signature. From the experimentation, it was clear that the proposed approach attained minimum computation and various significant properties.

In 2019, Mandala and Rao [2] have developed AAP-CSA model for preserving the data which was accomplished in two phases such as sanitization and restoration. In addition to this, an optimized key was produced to preserve secrecy. The simulation analysis verified the efficiency of the AAP-CSA through a comparative study over conventional models.

In 2019, Sun et al. [3] have established a data privacy preservation technique using k-anonymity-based approach to solve the location privacy issues. In this model, the LBSNs was utilized to produce dummy location using dummy-location selection model which was used to hide the customer's location. The extensive simulations revealed the performance of this system.

In 2019, Kim et al. [4] have presented a data privacy preservation approach using k-anonymity method to gather the personal information securely. This method utilized new protocols for data gathering and does not need any private channels. Moreover, a greedy heuristic model was proposed to handle the dynamic data holders as well as potential attacks. Through the simulation work, the efficiency of the protocols was examined.

In 2019, Gong et al. [5] have addressed a data privacy preservation approach via private regression analysis named PrivR to attain the goal by converting the format of polynomial as well as perturb the polynomial coefficients with respect to relevance among input and output features. The simulation study revealed the efficiency of PrivR by analyzing the bank dataset in terms of data leakage.

3. Objective Function of Proposed Data Sanitization and Restoration Process

3.1 Objective Function

Eq. (1) shows the fitness function of the adopted OI-CSA for achieving the privacy preservation of data.

$$\min \mathrm{F} = \max(\mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3, \mathrm{F}_4) \tag{1}$$

The fitness $\mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ and F_4 in Eq. (1) reveals the significance of the fitness functions and the following equations describe them as given below.

$$\mathrm{F}_1 = \frac{\mathrm{f}_1}{\max(\mathrm{f}_1)\forall \text{iterations}} \tag{2}$$

$$F_2 = \frac{f_2}{\max(f_2)\forall \text{iterations}} \tag{3}$$

$$F_3 = \frac{f_3}{\max(f_3)\forall \text{iterations}} \tag{4}$$

$$F_4 = \frac{f_4}{\max(f_4)\forall \text{iterations}} \tag{5}$$

In Eq. (2), F_1 indicates the standardized HF rate, f_1 points to the HF rate and $\max(f_1)$ is taken as the worst f_1 of the entire iterations. In Eq. (3), F_2 refers to the standardized MD rate, and f_2 represents the MD. In Eq. (4), F_3 specifies the standardized IP rate and f_3 portrays the IP rate and In Eq. (5), F_4 indicates the standardized rate of FR, f_4 refers to the FR. Furthermore, O specifies the original database and O' points to the sanitized database.

HF rate: The HF rate specified through f_1 can be explained as the part of sensitive rules that are represented in O' is stated in Eq. (6), in which, B specifies the association rule generated by concerning B' indicates the association rules attained using O' and sensitive rules is mentioned by SRs. Moreover, the sensitive rule count in O' can be stated as $f_1 = \left|B' \cap SRs\right|$.

$$f_1 = \frac{\left|B' \cap SRs\right|}{\left|SRs\right|} \tag{6}$$

IP rate: The IP rate indicated through f_2 can be expressed as "the rate of non-sensitive rules that are covered in O'". Usually, it is the inverse of loss of information which is portrayed in Eq. (7).

$$f_2 = 1 - \frac{\left|B - B'\right|}{\left|B\right|} \tag{7}$$

FR: Eq. (8) express the FR represented through f_3 which can be stated as "the rate of synthetic rules created in O'".

$$f_3 = \frac{\left|B - B'\right|}{\left|B'\right|} \tag{8}$$

DM: The DM pointed through f_4 can be represented as the modification count implemented in O' from O as revealed in Eq. (9), and $dist$ indicates the Euclidean distance among O' and O.

$$f_4 = dist(O, O') \tag{9}$$

3.2 Proposed Architecture

Fig. 1 depicts the complete architecture of proposed OI-CSA algorithm. At first, the data preservation model contains 2 prime phases such as sanitizing of data and restoring of data. Generally, in data sanitization model, there is a need for an efficient key which can be utilized to hide the data at the sender side, such that the sensitive data can be secured. For this purpose, the key is produced with the efficacy to hide the data perfectly so that the data can be safely transmitted. With the intension achieving this objective, the proposed OI-CSA model is implemented for optimum key creation. On the other hand, at the receiver side, only the authenticated candidate can restore the sanitized data through a similar optimal key.

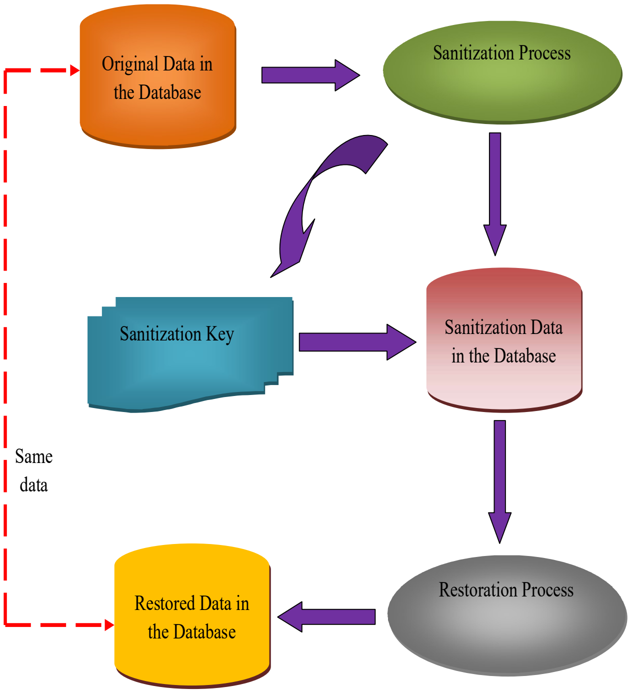

Original Data in the Database
Sanitization Process
Sanitization Key
Sanitization Data in the Database
Same data
Restored Data in the Database
Restoration Process

Fig. 1. *Adopted Data Privacy Preservation Framework*

3.3 Sanitization Process

In the sanitization model, the pruned key matrix A_2 and binarization of O are determined. The binarized format of the resultant key matrix is successively given into the rule hiding procedure where XOR operation is applied in the binarized format of O using the same matrix dimensions and summed with one which creates the O' as expressed in Eq. (10). In addition to this, the value of O' attained through the sanitization procedure accomplishes SRs and the association rules continuing the B'. Likely, O derives the comparative association rules preceding to sanitization B to achieve the objectives. Fig. 2 illustrates the graphical design of the proposed sanitization procedure.

$$O' = (A_2 \oplus O) + 1 \tag{10}$$

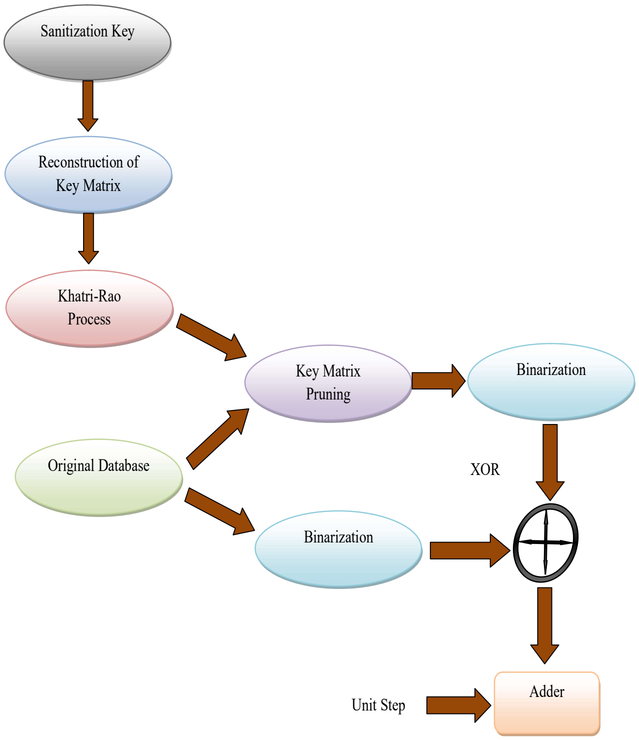


Fig. 2. *Graphical Demostration of Sanitization Procedure of the adopted PPDM System*

3.4 Key Generation

Usually, the key generation contains solution modification procedure, in which A specifies the key representation which is transformed using the help of khatri-Rao product. Initially, A is reorganized as A_1 and the matrix dimensions $\left[\sqrt{M_O''} \times O_{max}\right]$ in which O_{max} denotes the maximum transaction length M_O points to the number of transactions, the nearest maximum perfect square of M_O is represented as M_O''. i.e. the remodelled procedure of $A = \{1,2,1\}$ applies "row-wise duplication" and creates the reconstructed key matrix, A_1 with dimension $\left[\sqrt{M_O''} \times O_{max}\right]$ as stated in Eq. (11).

$$A_1 = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix}_{\left[\sqrt{M_O''} \times O_{max}\right]} \tag{11}$$

Therefore, A_2 with size $\left[\sqrt{M_O} \times O_{max}\right]$ is achieved using the Khatri-Rao product of 2 similarly reorganized A_1 matrixes which are indicated as $A_1 \otimes A_1$, where kronecker product is represented as $\otimes$ and its sizes were minimized based on original database. The key generating method is implemented and produces a matrix with size equal to O that produce $A_{2\left[\sqrt{M_O} \times O_{max}\right]}$ using Khatri-Rao product. At last, the procedure of rule hiding is performed to attain O' via sensitive rule hiding. The optimum creation of key is accomplished in terms of the enhanced CSA model named OI-CSA.

3.5 Restoration Process

In data restorating procedure, the O' attained through sanitization method and A_2 through key creation approach is binarized. In unit step input, the binarized S_d through binarization block can be reduced. Meanwhile, the binarized database and key matrix undergo an XOR operation which continues the subtraction and then the restored database is taken out. Eq. (11), Eq. (10), Eq. (1) and adopted OI-CSA update is utilized to reorganize the sanitizing key A_2.

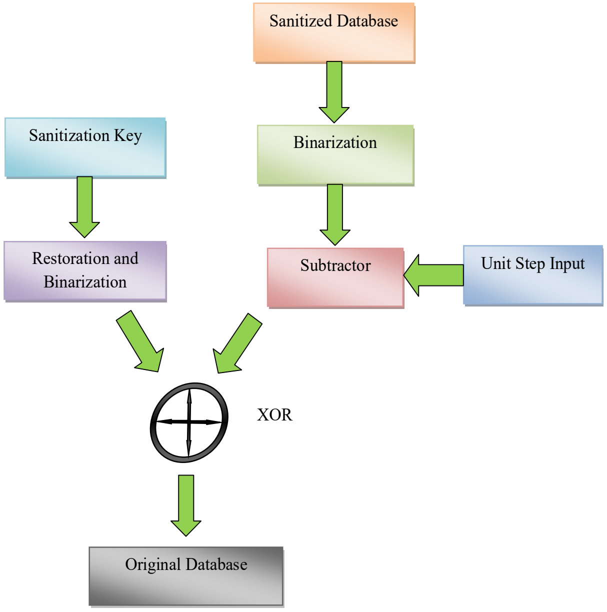


Fig. 3. *Restoration Procedure of adopted PPDM Model*

Moreover, all these equations are applied to produce O' through the lossless restoring that can be accomplished using the EQ. (12).

$$\hat{O} = \left(O' - 1\right) \oplus A_2 \tag{12}$$

In Eq. (12), $\hat{O}$ refers to the restored data. Fig. 3 depicts the structure of the restoration procedure.

4. Key Encoding: An Enhanced Approach

4.1 Key Encoding

Generally, the keys are considered as chromosome A which is utilized for the sanitization procedure. These keys are given to the proposed OI-CSA to encode the chromosomes. The number of chromosomes lies in the interval of A^1 to A^M which is optimized by the adopted method. Thereby, the optimum key is attained and the key length is given as $\sqrt{M_O''}$. Fig. 4 demonstrates the solution encoding of proposed OI-CSA model.

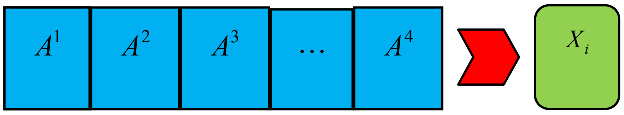


Fig. 4. *Keys for encoding*

4.2 CSA Model

Typically, the CSA [16] scheme is an approach mainly introduced based on the reproduction of Cuckoos. Further, the local and global arbitrary walks are defined in Eq. (14) and Eq. (13) respectively. In Eq. (13), X_i^t and X_k^t represents the present positions chosen through arbitrary permutation, β specifies the “positive step size scaling factor”, X_i^{t+1} refers to the following position, s portrays the size of step, $\otimes$ points to the “element-wise product of two vectors”, F indicates the “heavy side function”, P represents a constraint which is utilized to shift amongst global and arbitrary walks, ε refers to an random constraint. Moreover, in Eq. (14), $N(s,\tau)$ specifies levy distribution.

$$X_i^{t+1} = X_i^t + \beta s \otimes F(P-\varepsilon) \otimes \left(X_i^t - X_k^t\right) \tag{13}$$

$$X_i^{t+1} = X_i^t + \beta N(s,\tau) \tag{14}$$

4.3 OI-CSA Algorithm

Generally, the traditional CSA model is effectual in optimization problem solving and useful in complex engineering problems. However, the performance is limited when explicitly employed to solve multi-optimization issues. Thus, the conventional CS model is enhanced by changing the opposition intensity γ as defined in Eq. (15). Initially, in the traditional CSA, Eq. (14), X_i^t and $X_i^{(w)}$ portrays the current and worst solution and γ lies in 0 to 1. In order to attain Eq. (15), the step size is determined as given in Eq. (16), where c_s specifies the current solution, b_s indicates the best solution, r is a random number and co is a constant. Algorithm 1 shows the pseudocode of OI-CSA algorithm.

$$X_i^{t+1} = X_i^t + \beta N(s,\tau) - \gamma\left[X_i^{(w)} - X_i^t\right] \tag{15}$$

$$s = 0.01 \times step \times \left(c_s - b_s\right) \tag{16}$$

$$step = \frac{u}{abs(v)\left(\frac{1}{\beta}\right)} \tag{17}$$

$$u = r * \sigma \tag{18}$$

$$v = r \tag{19}$$

$$\sigma = \left(co(1+\beta) * \frac{\sin\left(\pi * \frac{\beta}{2}\right)}{co\left(\frac{1+\beta}{2}\right) * \beta * 2^{\frac{\beta-1}{2}}} \right)^{\frac{1}{\beta}} \tag{22}$$

Algorithm 1: Pseudo code of OI-CSA

```
Initialization
While $(t < \text{Max Generation})$ or end the process
    Portray a cuckoo (assume $i$) randomly;
    Compute its fitness ; $F_i$
    Select a nest amongst $n$ (assume $j$) randomly;
    Compute its fitness; $F_j$
    If $(F_i > F_j)$
        Update the solution as per Eq. (13);
    else
        Portray $\gamma$
        Update the solution as per Eq. (15)
    End if
    New nests are constructed at new sites
    Sustain the best solutions;
    Rank and portray the best;
End while
End
```

5. Result and Discussion

5.1 Simulation Procedure

The adopted OI-CSA approach for preserving the sensitive data has been executed in JAVA, and the outcomes were achieved. The examination was implemented through 4 datasets such as “T10, Chess, Retail, and T40”. In addition, the performance of the proposed OI-CSA was depicted through an algorithmic analysis by varying the co value for the four datasets. Moreover, the algorithmic analysis was implemented by concerning the hiding failure, information loss, and false rule generation for all the four datasets.

5.2 Algorithmic Analysis by varying co of OI-CSA

In this section, the algorithmic analysis for the effect of varying co through the Chess dataset is tabulated in Table 1. The co values vary in terms of 0.2, 0.4, 0.6, 0.8 and 1. In Table 1, the normalized MD rate F_2 is obtained as 0.482129, 0.482071, 0.482043, 0.48141, and 0.481148 for the co values of 0.2, 0.4, 0.6, 0.8 and 1 in order. In Table 2, for retail dataset, the normalized HF rate F_1 is obtained as 0.3685, 0.36575, 0.35225, 0.351, and 0.3505 for the co values of 0.2, 0.4, 0.6, 0.8 and 1 respectively. The normalized IP rate F_3 is derived the values of 0.2259, 0.190528, 0.184523, 0.166961, and 0.063881 for the corresponding co values of 0.2, 0.4, 0.6, 0.8 and 1 for T40 dataset is summarized in Table 3. In Table 4, for T10 dataset, the normalized FR rate F_4 is obtained as 0.221493, 0.190495, 0.189527, 0.183136, and 0.134694 for the corresponding co values of 0.2, 0.4, 0.6, 0.8 and 1. Hence, the efficiency of the adopted OI-CSA was revealed proficiently.

***Table 1.** Overall Analysis of the adopted scheme with respect to Varying co for Chess Dataset*

Measures	co =0.2	co =0.4	co =0.6	co =0.8	co =1
F_1	0.3685	0.36575	0.35225	0.351	0.3505
F_2	0.482129	0.482071	0.482043	0.48141	0.481148
F_3	0.196904	0.178222	0.145779	0.126728	0.113247
F_4	0.18456	0.182667	0.162154	0.154041	0.139631
F	0.482129	0.482071	0.482043	0.48141	0.481148

Table 2: *Overall Analysis of the adopted scheme with respect to Varying* co *for Retail Dataset*

Measures	co **=0.2**	co **=0.4**	co **=0.6**	co **=0.8**	co **=1**
F_1	0.25425	0.25175	0.25125	0.25075	0.017311
F_2	0.487782	0.487758	0.487734	0.487615	0.484474
F_3	0.199872	0.123455	0.107469	0.105863	0.094832
F_4	0.206573	0.127251	0.111925	0.110444	0.09835
F	0.487782	0.487758	0.487734	0.487615	0.484474

Table 3: *Overall Analysis of the adopted scheme with respect to Varying* co *for T40 Dataset*

Measures	co **=0.2**	co **=0.4**	co **=0.6**	co **=0.8**	co **=1**
F_1	0.2605	0.254	0.252	0.25125	0.24825
F_2	0.48825	0.488108	0.488084	0.487964	0.487655
F_3	0.2259	0.190528	0.184523	0.166961	0.063881
F_4	0.234151	0.203873	0.199073	0.174138	0.063061
F	0.48825	0.488108	0.488084	0.487964	0.487655

Table 4: *Overall Analysis of the adopted scheme with respect to Varying* co *for T10 Dataset*

Measures	co **=0.2**	co **=0.4**	co **=0.6**	co **=0.8**	co **=1**
F_1	0.24975	0.24925	0.24875	0.24825	0.036633
F_2	0.477638	0.477595	0.477552	0.477508	0.475339
F_3	0.210418	0.181734	0.174603	0.170139	0.124564
F_4	0.221493	0.190495	0.189527	0.183136	0.134694
F	0.477638	0.477595	0.477552	0.477508	0.475339

6. Conclusion

In this paper, an advanced model for data privacy preservation was proposed using the efficiency of the metaheuristic algorithm. Initially, a new PPDM approach has been devised through two phases such as data sanitizing and data restoring process that utilizes the efficiency of association rules. Generally, key creation is an essential step in data preservation which was formulated as an optimization problem and the optimal key was created using the adopted OI-CSA scheme. Moreover, the objective is to reduce the HF rate, IP, and FR and DM rate in order to achieve efficient data preservation method. Additionally, an algorithmic analysis was done to reveal the betterment of OI-CSA scheme. Here, the efficiency was improved by varying the co values in terms of 0.2, 0.4, 0.6, 0.8 and 1 in order for the datasets like chess, retail, T40, and T10. Moreover, the performance of proposed OI-CSA for the normalized MD rate F_2 was obtained as 0.482129, 0.482071, 0.482043, 0.48141, and 0.481148 for the co values of 0.2, 0.4, 0.6, 0.8 and 1 in order. Furthermore, the normalized IP rate F_3 is derived the values of 0.2259, 0.190528, 0.184523, 0.166961, and 0.063881 for the corresponding co values of 0.2, 0.4, 0.6, 0.8 and 1 for T40 dataset. Hence, the performance of the proposed data preservation model attained competitive results and revealed its efficiency in a proficient way.

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] C. Niu, Z. Zheng, F. Wu, X. Gao and G. Chen, "Achieving Data Truthfulness and Privacy Preservation in Data Markets," IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 1, pp. 105-119, 1 Jan. 2019.

[2] Jyothi Mandala, and M. V. P. Chandra Sekhara Rao, "Privacy preservation of data using crow search with adaptive awareness probability", Journal of Information Security and Applications, vol. 44, pp 157-169, February 2019.

[3] Gang Sun, Liangjun Song, Dan Liao, Hongfang Yu, and Victor Chang, "Towards privacy preservation for “check-in” services in location-based social networks", Information Sciences, vol. 481, pp 616-634, May 2019.

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

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

[6] L. Ni, C. Li, X. Wang, H. Jiang, and J. Yu, "DP-MCDBSCAN: Differential Privacy Preserving Multi-Core DBSCAN Clustering for Network User Data," IEEE Access, vol. 6, pp. 21053-21063, 2018.

[7] B. Shao, G. Bian, X. Quan, and Z. Wang, "Research of privacy preservation method based on data coloring," China Communications, vol. 13, no. 10, pp. 181-197, Oct. 2016.

[8] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao and Z. Huo, "Privacy Preservation in Big Data From the Communication Perspective—A Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 753-778, Firstquarter 2019.

[9] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin and K. Ren, "Real-Time and Spatio-Temporal Crowd-Sourced Social Network Data Publishing with Differential Privacy," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 591-606, 1 July-Aug. 2018.

[10] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin and X. Shen, "Morality-Driven Data Forwarding With Privacy Preservation in Mobile Social Networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 7, pp. 3209-3222, Sept. 2012.

[11] X. Zhang, C. Liu, S. Nepal, S. Pandey, and J. Chen, "A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1192-1202, June 2013.

[12] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A Framework for Categorizing and Applying Privacy-Preservation Techniques in Big Data Mining," Computer, vol. 49, no. 2, pp. 54-62, Feb. 2016.

[13] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez and S. Martínez, "t-Closeness through Microaggregation: Strict Privacy with Enhanced Utility Preservation," IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 11, pp. 3098-3110, 1 Nov. 2015.

[14] J. He, L. Cai and X. Guan, "Preserving Data-Privacy With Added Noises: Optimal Estimation and Privacy Analysis," IEEE Transactions on Information Theory, vol. 64, no. 8, pp. 5677-5690, Aug. 2018.

[15] X. Wang, J. He, P. Cheng and J. Chen, "Privacy Preserving Collaborative Computing: Heterogeneous Privacy Guarantee and Efficient Incentive Mechanism," IEEE Transactions on Signal Processing, vol. 67, no. 1, pp. 221-233, 1 Jan.1, 2019.

[16] M. Mareli, and B. Twala, "An adaptive Cuckoo search algorithm for optimisation", Applied Computing and Informatics, vol. 14, no. 2, pp 107-115, July 2018.