Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549433

PRIVACY PRESERVATION IN CLOUD USING GLOWWORM SWARM-BASED WHALE OPTIMIZATION ALGORITHM (GWOA) & 2D IIR FILTER IN HUNGARIAN DATASET WITH 128 KEY SIZE

Reshma Nitin Atole
Assistant Professor, Department of Computer Science and Engineering, Shivnagar Vidya Prasarak Mandal's College of Engineering, Baramati, Pune, India.
reshma174@gmail.com

Abstract: - *Cloud Computing is the novel system for sharing various resources through internet. Cloud technology is the supply of various services it includes storage, database, connectivity, software, analytics and intellectual service. This technology eliminates the capital expense of buying software and also hardware. Many cloud service providers present a large set of set of privacy policies and terms to the cloud users. Privacy means securing data from being used by others. Many organizations stored their information on the cloud. Health care organizations save their patient's data on the cloud due to their reliability. These patients's information is very sensitive. This research work uses GOWA algorithm to preserve the patient's data safely. Stored data can be filtered by using 2D IIR filter. The data are transferred from one cloud to another while the data is protected by GOWA algorithm. This research work GOWA algorithm plays a major role for preserving the patient's data in a secured manner in cloud environment. Analysis of the proposed GWOA algorithm using Hungarian dataset with 128 key size for the metrics, like utility and privacy.*

Keywords: - *GOWA Algorithm, 2D IIR Filter, Privacy Preservation, Data Base, Hungarian dataset*

I INTRODUCTION

Another name of Cloud computing is known as virtual computing in current communication technology. It makes various data centers used to store large volume of data. But security and privacy preservation are the key issue in cloud concept. Privacy preservation means the sensitive data should to discharge to the third party people during data transmission. Many cloud computing service providers uses various encryption methods for privacy over the cloud stored data. Using encrypting methods the patient's health related sensitive information can be stored on the cloud. Important issues in cloud environment are integrity of information, confidentiality of patient information, availability of patient data and privacy of patient data. The following figure 1 shows the various privacy issues available in the cloud storage. To avoid such kind of privacy issues in this research GWOA algorithm is used. The main goal of this proposed concept is to preserve the patient's health data in secure manner. The preserved data can be stored on the cloud. From the cloud storage the users can able access the information in any time at anywhere using internet.

The remaining of this research article is classified as: Section 2 describes various technologies to preserve privacy data. Section 3 elaborates the proposed algorithm used for privacy preservation section 4 discusses about the result of proposed algorithm using Hungarian dataset. Finally, section 5 concludes the research paper.

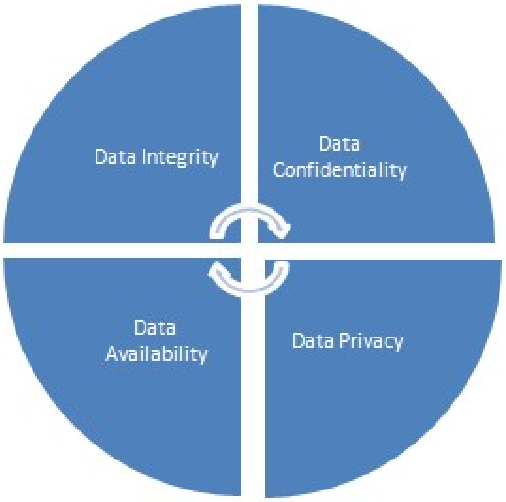


Figure 1 Important Privacy Problems in Cloud Environment

II LITERATURE REVIEW

Many business organizations earning maximum profit using this cloud computing technology. But privacy preservation is the major problem in this cloud environment. Encryption and decryption concepts are playing major role in cloud storage system. Jayashree Agarkhed et al., presented various security related issues in cloud. They said that cryptographic concepts are used to safely store information on the cloud. RSA security algorithm combined with DES algorithm to preserve patient’s data in cloud storage [1].

Cloud computing provides various computing resources based on user’s demand. Users can pay the amount based on their usage. Cloud environment allows to store patient’s sensitive data also. Security is the major concern in healthcare sensitive data because large volume of data stored. Rayapati Venkata Sudhakar et al., provided quasi-identifier for anonymized data based on index value for preserving large amount of data to improve the efficiency of existing approaches [2].

Cloud computing users are needed to store the data in secure manner. Privacy means the specific data cannot be accessed by the third party users. Various security algorithms like AES, RSA and MD5 are used to provide better security in cloud computing environment. Mohammed Faez Al-Jaberi et al., studied about various security algorithms and proposed a new framework. It provides information privacy preservation in cloud [3].

Chandramohan.D et al., constructed a new layered architecture to secure the data on the cloud. This model is used to prevent data loss on cloud. Using this architecture the data can be encrypted using onion encryption concept. This new framework is called as onion and garlic architecture. It issues better back using encryption and decryption concept to manage privacy when hackers are try to access the cloud data [4].

Hong Liu et al., developed a new preservation technique. This technique is used on wearable materials. In this research work the authors designed a cooperative privacy preservation concept for human wearable products. In this concept identity verification and access control are taken to considerations with space related and time related factors. In space related mode

Minhash algorithm is used for improve the privacy level in sensitive data and detecting the similarity between patient's data. In time aware mode ciphertext concept is used for access control. To attain organized data using bloom filter technique. Mainly bloom filter is used to check current values stored in secret format or not [5].

III PROPOSED GLOWWORM SWARM-BASED WHALE OPTIMIZATION ALGORITHM FOR PRIVACY PRESERVATION IN CLOUD

Cloud contains large volume of data. Healthcare organizations also store the patient's details on the cloud environment because it provides large volume of storage space. But privacy is required for protecting patient's data on cloud. This research work performs the privacy concept in cloud by using new GWOA concept. It consists of various stages. In the first stage patient's medical data can be collected. Filtering concepts are applied in the second stage of this process. Here 2D IIR filter is used to filter the patient's health data. Filter coefficients are used to generate privacy data. In the third stage GWOA algorithm is applied in the filtered data. The output of the GWOA algorithm can be stored on database in fourth stage. Data can be move to the cloud in the fifth stage. From the cloud the users can able to access the preserved data. Figure 1 shows the various stages of the proposed GWOA-based privacy preservation model.

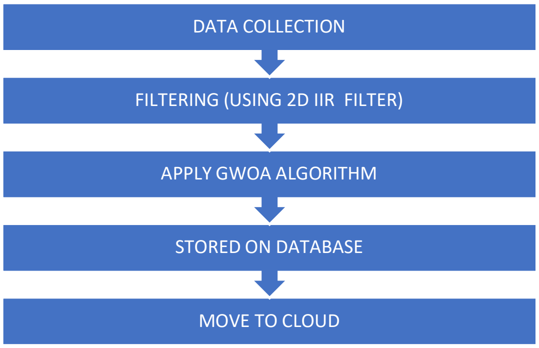


Figure 2 Various Stages of Proposed System

PROPOSED GWOA ALGORITHM

These are the following steps used in GWOA algorithm:

1. Population initialization
2. Specify the step size
3. Generate the glowworm agents randomly
4. set the maximum number of iteration
5. compute the luciferin update phase for each glowworm
6. compute the movement phase for each glowworm
7. compute the glowworm movements

IV. RESULTS AND DISCUSSION

The results of designed GWOA concept are explained in this part. Performance of the GOWA approach is measured using the important two metrics, such as privacy, and utility, respectively.

4.1 Evaluation metrics

The performance of the proposed algorithm is evaluated using the performance metrics, like privacy, and utility.

Privacy: It is defined as the ratio of difference between the filter vectors, which is given by,

$$A = \frac{\tau_a . \tau_b}{\tau_a + \tau_b - \tau_a . \tau_b} \qquad (1)$$

where, τ_a and τ_b are the two filter vectors.

Utility: It is a measure computed using the filter vectors, which is expressed as,

$$M = \frac{A + C}{T} \qquad (2)$$

where, A represents the true positive value, C represents the true negative value, and T represents the total measure, respectively.

Analysis using Hungarian dataset with 128 key size

Figure 3) demonstrates the analysis of the metrics privacy and utility by varying the training percentage level using Hungarian dataset with 128 key size.

Figure 3 a) demonstrates the analysis of privacy metrics based on training percentage value. When training percentage value is equal to 50%, the privacy metrics is collected by GWOA is 0.2231. The improved percentage reported when comparing the proposed method with existing methods GA, WOA, RGADP, and BSWOA is 72%, 38%, 27%, and 23%. When training percentage value is 60%, the privacy metrics of the GWOA is 0.2115.

The percentage value reported when comparing the proposed method with the existing methods GA, WOA, RGADP, and BSWOA is 76%, 60%, 15%, and 13%. When training percentage value is70%, the privacy metric value is obtained by the existing methods GA, WOA, RGADP, and BSWOA is 0.1160, 0.1402, 0.1458, and 0.1657, whereas the GWOA produces better privacy metric value of 0.2217. When training percentage level is 80%, the privacy value is received by the existing methods GA, WOA, RGADP, and BSWOA is 0.1033, 0.1243, 0.1278, and 0.1891, whereas the GWOA provides better privacy of 0.2271.

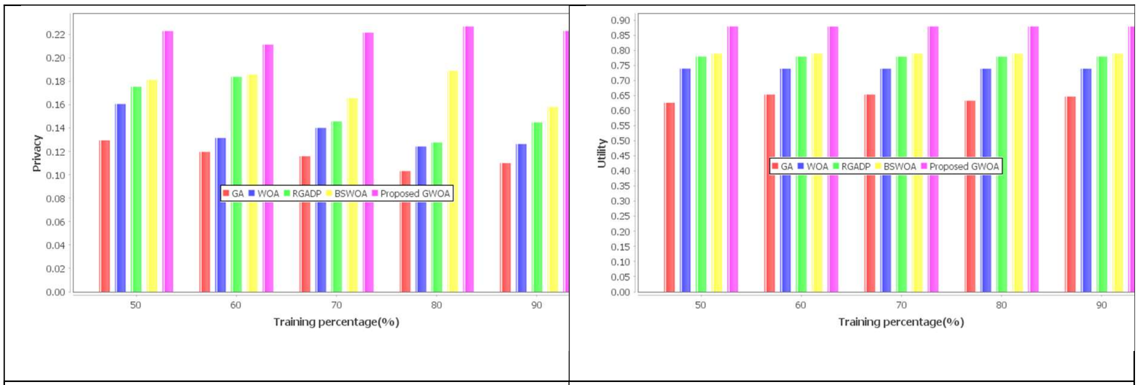
When training percentage value is 90%, the privacy metric value is get by the GWOA is 0.2232. The improved percentage value is reported when comparing the proposed method the existing methods GA, WOA, RGADP, and BSWOA is 96%, 76%, 54%, and 41%.

Figure 3 b) demonstrates the analysis of utility metric with respect to the training percentage level. When training percentage value is equal to 50%, the utility metric is obtained by the GWOA is 0.8785. The improved value reported when comparing the proposed method with existing methodse GA, WOA, RGADP, and BSWOA is 40%, 18%, 12%, and 11%.

When training percentage value is 60%, the utility metric is attained by the GWOA is 0.8783. The improved percentage is reported when comparing the proposed method with existing methods GA, WOA, RGADP, and BSWOA is 34%, 18%, 12%, and 11%. When training percentage is 70%, the utility metric derived by the existing methods GA, WOA, RGADP, and

BSWOA is 0.6531, 0.7387, 0.7785, and 0.7886, whereas the GWOA produced better utility metric value of 0.8786.

When training percentage level is 80%, the utility metric collected by the existing methods GA, WOA, RGADP, and BSWOA is 0.6327, 0.7387, 0.7784, and 0.7886, while the GWOA concept attained better utility metric 0.8786. When training percentage value is equal to 90%, the utility metric obtained by GWOA is 0.8783. The improved percentage value reported when comparing the proposed method with the existing methods GA, WOA, RGADP, and BSWOA is 35%, 18%, 12%, and 11%.



(a) **(b)**

Figure 3 Comparative analysis using Hungarian dataset with 128 key size, a) privacy, b) utility

V CONCLUSION

Cloud computing provides various computing resources based on user's demand. Users can pay the amount based on their usage. Various approaches are used to guard the data on the cloud system. This current digital world various open communication channels are available. Due to these open channels various security issues are occurred. To avoid privacy issue in this research work uses GWOA algorithm. Compare with other privacy approaches, this proposed method provides better result in terms of privacy and utility. In this research paper the proposed algorithm tested with Hungarian dataset with 128 key size. This proposed GWOA algorithm exposed the higher performance level using the metrics privacy and utility with the obtained values 0.2232 and 0.8783.

REFERENCES

[1] Jayashree Agarkhed & Ashalatha R. (2017), " A privacy preservation scheme in cloud environment.", 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), IEEE.

[2] Rayapati Venkata Sudhakar & T. Ch. Malleswara Rao (2016), " Index based quasi-identifier approach for privacy preservation data sets on cloud", 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Publisher: IEEE.

[3] Mohammed Faez Al-Jaberi & Anazida Zainal (2014), “Data integrity and privacy model in cloud computing.”, 2014 International Symposium on Biometrics and Security Technologies, IEEE, pp. 280-284.

[4] Chandramohan, D., Vengattaraman, T., Rajaguru, D., Baskaran, R., & Dhavachelvan, P. (2013), “A novel framework to prevent privacy breach in cloud data storage area service.”, 2013 International Conference on Green High Performance Computing (ICGHPC).

[5] Hong Liu, Xuanxia Yao, Tao Yang & Huansheng Ning (2018), “ Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing Based Smart Health”, IEEE Internet of Things Journal, pp 1-11.

[6] Gaofeng Zhang , Yun Yang , Xuyun Zhang , Chang Liu & Jinjun Chen (2012), “Key Research Issues for Privacy Protection and Preservation in Cloud Computing” 2012 Second International Conference on Cloud and Green Computing.

[7]. Keshanchia, B. Souria, A. & Navimipourb, N.J(2017). “An improved genetic algorithm for task scheduling in the cloud environments using the priority queues: formal verification Simulation, and Statistical testing”, Journal of Systems and Software, vol. 124, pp. 1–21.

[8] Revathi, S.T., Ramaraj, N. and Chithra, S.(2018), “Brain storm-based Whale Optimization Algorithm for privacy-protected data publishing in cloud computing”, Cluster Computing, pp.1-10.

[9]S. Nirmala Sugirtha Rajini & E. Mercy Beulah (2016), “Cloud Based Architecture For Healthcare System”, Asian Journal of Microbiology, Biotechnology and Environmental Sciences, Vol. 18, No. (4) , pp. 1017-1018.

[10] Mirjalili S. & Lewis A(2016), “The whale optimization algorithm”, Advances in Engineering Software, 95, pp.51-67.

[11] Cleveland, Hungarian & Switzerland database from UCI machine learning repository, “https://archive.ics.uci.edu/ml/datasets/Heart+Disease”, accessed on August 2019.

[12] Pinkas, B.(2002), “Cryptographic techniques for privacy-preserving data mining”, ACM Sigkdd Explorations Newsletter, vol. 4, no. 2, pp.12-19.

[13] Lu, R., Liang, X., Li, X., Lin, X. & Shen, X.(2012), “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications”, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp.1621-1631.