Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549444

ENHANCING PRIVACY CONTROL IN CLOUD COMPUTING BY GLOWWORM SWARM-BASED WHALE OPTIMIZATION ALGORITHM (GWOA) IN HUNGARIAN DATASET WITH 256 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: - Many organizations are ready to adopt current communication technology. Cloud service provides various virtual resources in term of hardware and software. It provides large amount of storage space to store large volume of organizations data. Healthcare organizations transferred their patient's data from local server system to cloud storage. But security is the major problem in cloud storage. So in cloud all the data is stored but at the same time privacy of data in health sector is very important. In the health sector sometime there is a need to take only some specific data. So this research here 2DIIR filter is used to filter the only required messages. 2D IIR filter is the two dimensional filters. The Privacy of the patient data is done using GOWA algorithm in the cloud environment. Analysis of the proposed GWOA algorithm using Hungarian dataset with 256 key size for the metrics, like utility and privacy.

Keywords: - Cloud Computing, Privacy Preservation, GWOA Algorithm, 2D IIR Filter, Hungarian dataset

I INTRODUCTION

Cloud relies on the sharing of the resources to achieve the coherence. Cloud computing is the technology which uses the central data. This technology allows the users to utilize the various resources at any computer with internet access. In simple words cloud refers to the storing and accessing data and programs over the internet instead of storing in the local computer's hard drive. Business peoples are earning more profit using this cloud concept. From the wearable smart devices patient's sensitive data can be collected. Data privacy and sensibility are the major issue in cloud environment due to open communication channel. Though cloud computing provides a secured environment, the data are also encrypted using RSA algorithm in advance to ensure security. RSA algorithm includes public and private keys. To obtain secured storage of health care data, service providers uses symmetric encryption and Attribute-Based Encryption. Cloud concept has reduced the labor to collect, input and analyze data. As real time data provider, cloud computing has become the network with pay-as-you-go pricing allowing us to create, configure, and customize data. End-to-end data encryption restricts data access by illegal users and provides privacy for designated recipients. This research work proposes a new GWOA algorithm to improve the privacy control in cloud computing environment to store patient's sensitive data.

The remaining part of this paper is organized as: Section 2 describes various methods and concepts are used to preserve patent's information. Section 3 elaborates the challenges faced by the cloud service providers. Section 4 deals with proposed algorithm used for privacy preservation section 5 discusses about the result of proposed algorithm using Hungarian dataset with key size 256. Finally, section 6 concludes the research paper.

II LITERTURE REVIEW

Nishitha Ramakrishnan et al., briefs that a significant challenge of managing the hospital data and maintenance of Patient Health Record (PHR) online is efficiently done by Cloud process. PHR stored in cloud can be assessed only after requesting the patient and the patient decides whether the source is a trusty one to grant the private key. It discusses with the modules involved in Hospital Management System (HMS). The modules are divided into Admin, Patient, hospital and doctor, therefore obtaining a scalable and secure data access control. This approach is open to both types of domains either open or closed domain. PHR's can be accessed by multiple security domains like Health care and Public. Some advantages involved in the proposed design of HMS are real time service provided by the doctors using PHR of the patient online and it is patient -centric concept which ensures the complete control of privacy to the patient. The unique challenge in the design is complexity of multiple PHR owners increasing the number of users [1].

Vijayakumar. V et al. Surveys and elaborates that computing services were provided as a utility and faced the challenge of lack in connectivity and bandwidth. To resolve this challenge computing services were upgraded to cloud technology which provides delivery of computing services in the form of servers, storage, databases, networking, software, analytics and more over the internet. It suggests that Searchable Symmetric Encryption (SSE) algorithm enhances and detects the security and privacy of the Patient's Health Record (PHR), Proxy Re-Encryption reduces the vulnerability of health care data, Attribute-based encryption provides public-key cryptography and Proofs of Retrievability technique ensures the client that all the appropriate data are stored and retrieved at any time. Additionally cloud concept has scope to detect the distribution of patient data illegally and diagnose the possible data leakage source of the authorized user [2].

Sujatha. R et al., reviews about evacuating duplication of health care records. It illustrates the importance of secrecy and security of the patient's information. Re-duplication of information such as X-rays and scan reports are managed proficiently with various authentications. Without decrease in quality, Re-duplication can be done. It proposes a system in which the patient's data are encrypted in to health record by the service provider or data owner. Duplication of files required more storage area in cloud. To ensure that only once data is entered into cloud environment, a detection scheme has been uploaded. A public key is provided to the patient by the data owners or service staffs of the hospital to access their health care files. MANHSP concept is used for re-duplication of patient's healthcare report and allows only authorized user to download and view the information in a secured manner. Though cloud concept is strong in security and privacy, now-a-days its storage cannot be trusted regardless of straightforward. Unapproved clients without substantial memberships are not capable to decrypt the information from cloud by themselves. Cryptographic hash function is used in a very secured way for information integrity. They suggest that reduplication of information helps to spare storage room, minimize transfer speed prerequisites, simple support for patient data, rapid recovery of information without any leakage in information to enhance the health care record secrecy and over cloud stockpiling [3].

Uthpala Premarathne et al., says that cloud concept deals with big data with three properties namely volume, velocity and variety. Managing such big data is identified as a threat when EHR based system is implemented poorly leading to stealing of data by unauthorized users. To improve the workflow and efficiency of healthcare service mobile devices are recommended. This study suggest that Electrocardiography (ECG) is a host signal that verify the security of data and to ensure it they propose a cryptographic role based access control that can handle multiple users. A Steganography based design is used to hide data securely, so that only authorized user can download data from the cloud. The approach details that Health service provider validates mobile users verifying their identity and location attributes. A domain server is consulted by the user for authentication, which moves to the health authority requesting to verify validation of the user and it informs the cloud system to permit the requested data to be transmitted. Thus ECG strengthens the secrecy of the healthcare data [4].

Wang, Y et al., has framed algorithms for consortium block chain to ensure the preserving of valuable health care data by the hospital management. Block chain technology provides a confident solution by its novel properties of, anonymity and verifiability. This protocol uses searchable encryption and conditional proxy re-encryption to ascertain data security and privacy. The proposed scheme achieves security goals and high computational efficiency. Block chain technology figure out security issues in sharing of healthcare record. The challenges in this system elongate to achieving data privacy preservation, realizing that only patient and authority can access data and in designing data structure and consensus mechanism. Cloud based block chain scheme addresses all the above challenges. Consensus mechanism means that using block chain as the way to reach consensus within untrustworthy nodes in the distributed environment. The study reveals a framework for sharing Electronic Health Records among different health institutes using cloud based block chain. Then network model, data structure and consensus mechanism are designed for the regular operation of the system. Further security analysis is done as a proof of providing quality performance [5].

III CHALLENGES IN PRIVACY PRESERVING

Storing patient's data on the cloud environment the cloud providers faces various challenges. The major challenges are described below.

Healthcare in cloud environment is raising attractiveness to store large volume of patient's data. But privacy and security is the important issue of the cloud providers.

Lacking of users access control is the major issue in healthcare sector.

Healthcare applications do not provide privacy data of the patients. It makes the healthcare system as unsecure.

Healthcare applications contain patient's sensitive data. Due to this reason cloud architecture in the medical system becomes more complex than other cloud applications.

IV PROPOSED METHODOLOGY

This research work is based on GWOA privacy preserving algorithm. The input medical data is collected from Hungarian dataset and develop the privacy preservation model using the GWOA algorithm. This proposed model provides more security in cloud environment. The users can access the protected data from the cloud environment. The following figure 1 shows the flow diagram of proposed model.

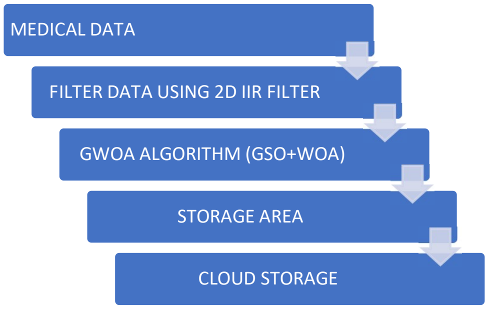


Figure 1 Process Flow of Proposed System

The collected input patient's health data is subjected to the filtering concept. Here 2D IIR filter is used for that filtering purpose. This filter generates a filter matrix. It contains filter coefficient. This filter coefficient is used in preservation procedure. The resulted filter matrix acquired using the filter response is mathematically described as,

$$E = \sum_{m_1=0}^{M_1-1} \sum_{m_2=0}^{M_2-1} f(m_1,m_2) D(i-m_1, j-m_2) - \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} g(n_1,n_2) E(i-n_1, j-n_2) \qquad (1)$$

Where, E represents the filter matrix having the dimension of $[b \times c]$, D is represented as the database. $f(m_1, m_2)$, and $g(n_1, n_2)$ are the filter coefficients, which are used in the proposed GWOA algorithm.

The filter vector Z with the single digit value is indicated as,

$$Z = \sum_{m_1=0}^{M_1-1} \sum_{m_2=0}^{M_2-1} f(m_1,m_2) + \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} g(n_1,n_2) \qquad (2)$$

PROPOSED GWOA ALGORITHM

GWOA algorithm is used to protect the patient's data in secured manner. It is the combination of Glowworm Swarm Optimization (GSO) and Whale Optimization Algorithm (WOA). The various algorithmic steps are used in the proposed GWOA algorithm are,

a) Solution encoding
b) Fitness evaluation
c) Glow-worm update phase
    i) Luciferin update phase
    ii) Movement phase
    iii) Neighbourhood update phase

d)Termination Phase

V RESULTS AND DISCUSSION

The experimentation of the proposed algorithm is carried out by the JAVA tool using, Hungarian database with 256 key size from UCI machine learning repository.

Analysis using Hungarian dataset with 256 key size

Figure 2 describes the analysis of privacy and utility metrics by varying the training percentage value using Hungarian dataset with 256 key size.

Figure 2 a) represents the analysis of privacy value with respect to the training percentage value. When the training percentage is equal to 50%, the privacy value is received by the proposed GWOA algorithm is 0.2225. The percentage of increased value reported when comparing posted method with existing methods GA, WOA, RGADP, and BSWOA is 97%, 67%, 52%, and 36%.

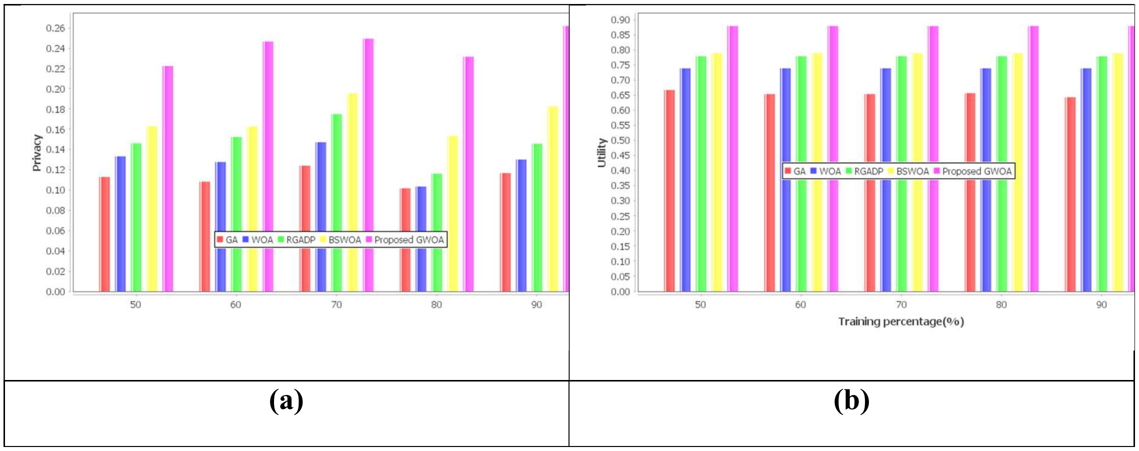
When training percentage value is 60%, the privacy value got by the proposed GWOA algorithm is 0.2465. Percentage value can be improved and reported when comparing the proposed method existing methods GA, WOA, RGADP, and BSWOA is 97%, 93%, 61%, and 51%. If training percentage value is equal to 70%, the privacy value got by the existing methods GA, WOA, RGADP, and BSWOA is 0.1241, 0.1472, 0.1750, and 0.1955, whereas the proposed GWOA provides better privacy of 0.2493.

Training percentage value is 80%, the privacy value attained by the existing methods GA, WOA, RGADP, and BSWOA is 0.1017, 0.1035, 0.1161, and 0.1535, whereas the proposed GWOA algorithm computes the better privacy of 0.2316. When training percentage value is equal to 90%, the privacy value collected by the proposed GWOA algorithm is 0.2619. The percentage level is improved and reported when comparing the proposed and existing methods GA, WOA, RGADP, and BSWOA is 94%, 91%, 79%, and 43%.

Figure 2 b) desribes the analysis of utility with respect to the training percentage level. When training percentage value is 50%, the utility value is obtained from GWOA concept is 0.8786. The percentage level can be increased and reported when comparing the proposed method and existing methods GA, WOA, RGADP, and BSWOA is 31%, 19%, 12%, and 11%. If the training percentage value is equal to 60%, the utility value is collected proposed GWOA algorithm is 0.8787.

The percentage value level is improved and reported when comparing the proposed and existing methods GA, WOA, RGADP, and BSWOA is 34%, 19%, 12%, and 11%. When training percentage value is 70%, the utility value collected by the existing methods GA, WOA, RGADP, and BSWOA is 0.6531, 0.7387, 0.7785, and 0.7886, whereas the proposed GWOA provides better utility of 0.8786. If training percentage equal to 80%, the utility value collected by the existing methods GA, WOA, RGADP, and BSWOA is 0.6531, 0.7385, 0.7786, and 0.7886, whereas the proposed GWOA issues better utility of 0.8786.

When training percentage level is 90%, the utility value received by the proposed GWOA concept is 0.8786. The percentage value can be improved and reported when comparing the proposed method with existing methods GA, WOA, RGADP, and BSWOA is 36%, 19%, 12%, and 11%,.



(a) **(b)**

Figure 2 Comparative analysis using Hungarian dataset with 256 key size, a) privacy, b) utility

VI CONCLUSION

Privacy is very important in health sectors. Patient's data is secured in the cloud environment. The patient's data is secured in a proper manner in the cloud by using GOWA algorithm. Some time there is a need to get only some specific and wanted data. 2DIIR filters are used to gain only some specific data. The data is exchanged between the cloud and the data is secured in a safe manner by GWOA algorithm. To overcome the privacy issue in cloud uses GWOA algorithm. This proposed concept provides improved result in terms of privacy and utility. In this research paper the proposed algorithm tested with Hungarian dataset with 258 key sizes. This proposed GWOA algorithm exposed the good performance using the metrics privacy and utility with the values of 0.2619 and 0.878.

REFERENCES

1. Nishitha Ramakrishnan & Sreerekha(2015), "Enhancing Security of Personal Health Records in Cloud computing by Encryption", International Journal of Science and Research (IJSR) , ISSN 2319-7064,Vol. 4, No. 4.

2. Vijayakumar.V, K. Premkumar, Sasirekha.N, Punithavalli.G & Deebika.G(2018), "Cloud computing on Health Care Management", International Journal of Pure and applied Mathematics, Vol. 118, No. 14 2018, pp. 547-555.

3. Sujatha. R & Kaviya. P.S 9(2017), "Optimizing Health care records by preventing duplication in cloud", International journal of Research in Pharmaceutical sciences, pp. 247-250

4. Uthpala Premarathne, Alsharif Abuadbba, and Abdulatif Alabdulatif, Ibrahim Khalil, Zahir Tari, Albert Zomaya, Rajkumar Buyya (2016)," Hybrid Cryptographic Access Control for CloudBased EHR Systems", IEEE cloud computing, pp. 58-64

5. Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019), " Cloud-Assisted EHR Sharing with Security and Privacy Preservation Via Consortium Blockchain", IEEE Access.
6. 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.

7. Mirjalili S. & Lewis A(2016), "The whale optimization algorithm", Advances in Engineering Software, 95, pp.51-67.

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

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