Data Protection Security Model In Cloud Computing Using Glowworm Swarm-Based Whale Optimized Framework

Yogita Deepak Sinkar
Dept. of Computer Science & Engineering
Bharath Institute of Higher Education and Research
Chennai, India
gtsinkar186@gmail.com

C.Rajabhushanam
Dept. of Computer Science & Engineering
Bharath Institute of Higher Education and Research Chennai, India
rajabhushanamc.cse@bharathuniv.ac.in

Abstract—
Preservation of security is urgently needed to minimize the disclosure of confidential patient data. Numerous methods of privacy protection are implemented in the cloud system, but in the cloud world, preserving personal data of the user is still a challenging problem. An important privacy protection policy must therefore be built to protect the user's medical data. The input medical data is initially obtained and introduced to the filter system to conduct the process of privacy protection. The filtering process is advanced using the 2D Infinite Impulse Response (IIR) filter which uses the filter factoring model to generate a filter matrix. The filtering matrix generated is used to create the data preserved for the security wherein the filter vector is focused on the planned Glowworm Swarm Whale Optimization Algorithm (GWOA), the Glowworm Swarm Optimization (GSO) and Whale Optimization Algorithm (WOA) integration. The data stored resulting in privacy is subjected to the data storage system, where the stored data is registered. Instead, the retained data is stored in the information environment's information management system to allow user access with greater privacy and utility. With higher privacy, the proposed algorithm achieved better quality and utility values of 0.2698 and 0.8786, accordingly when the key size is 256 when using Switzerland database.

Keywords— Filter factoring, vector filtering, Glowworm Swarm Optimization (GSO), web security

A. INTRODUCTION

Cloud computing is one of the latest technologies, which is gaining considerable attention in the field of industrial and academic research due to the rapid development in information and computer science technology [16]. It is known as the novel invented fusion of various ideas and technologies that essentially design business plans using economic sales via communication technology services [2][24] Cloud computing is generally characterized as a software-defined model and computing substructure that allows configurable storage pools to access strategy such as application services, computer networks, etc. However, it is a boost in the information technology (IT) milestone, so scientists and numerous researchers have confirmed cloud computing [1]. In addition, the services provided by the cloud computing platform are flexible and secure, as it includes Infrastructure as a Service (IaaS), Software as a

Service (SaaS), All as a Service (XaaS), even Platform as a Service (PaaS) [16][22]. It showed significant growth to enhance cooperation among various health care providers. Additionally, the transfer of big data from the medical institution into the cloud freed the health care system from the leadership activities. In general, the e-health cloud platform is highly developed to store and manage vast amounts of healthcare information between the provider [9][23]. Also though the cloud platform offers on-demand infrastructure, protecting privacy is a major barrier [16][20]. Healthcare cloud is the cloud system through which stakeholders and healthcare providers interact via cloud server [12][19]. In comparison, a cloud setting of the healthcare sector greatly offers a flexible and rational software platform, thus dispersing the medical professionals and the patients. Digital service is also allowed to promote collaboration between doctors, clinicians, and patients to address symptoms, medical problems, including treatments [14][21]. Security is the main element in the cloud and it has the sub-factor as anonymity necessary to remove the disclosure of responsive data [10][15] to patients. Preservation of privacy is an essential element in the approach to clinical prediagnosis because more sensitive material is found in the patient records. If adequate security of privacy is not specifically established, instead consumers oppose the assumption [2][11].

B. LITERATURE SURVEY

Alphonsa M.A. and Amudhavalli P [1] introduced a changed lightning bug formula to perform knowledge the info the information restoration and data cleansing method. It earned higher performance with reference to the key sensitivity and achieved effective restoration and cleansing framework. However, the correlation between the key and encrypted knowledge was terribly less. Karlekar N.P. and Gomathi N [2] sculptured a mathematician product and Bat formula to perform the privacy preservation method within the cloud surroundings. It effectively obtained the privacy preserved knowledge and earned higher DBDR and accuracy for corroborative the privacy live. However, it didn't attain a most range of iterations.

Tong Li et al. [3] introduced an information business approach to making rife records. It achieved a higher privacy protection method by conserving the integrity of information. It earned higher obscurity performance while not eliminating sensitive attributes. However, it had been applicable to a sophisticated business system.

Li J et al. [4] developed conserving multiparty information privacy (PMDP) approach to safeguard the numeric information and to publish the information in untrusted cloud. It effectively achieved the storage delegation at the same time and guarantees the protection while not collusion. However, it did not satisfy the strain of massive information.

Piao C et al. [5] developed a fog computing approach to business enterprise the information within the cloud. It uses the differential methodology to forestall the privacy from speech act. However, it reduced the sensitivity of queries and increased the utility of information business enterprise. Moreover, it did not reach information sharing at the fog layer. Song W et al. [6] introduced a text retrieval approach within the cloud paradigm. It effectively extracts the words from the contents within the documents. it absolutely was safer and privacy preserved over the cloud information. However, the analysis of risk wasn't thought-about over the attack situation. Wu Z et al. [7] developed a client-based privacy protection model within the cloud. {the information the info the information} before storing it to the cloud was encrypted exploitation associate encoding mechanism to reinforce the protection of the cloud data. It with efficiency dead the queries exploitation encrypted information. However, defend the information with the user behavior wasn't happy.

Rawal B.S et al. [8] sculptural a secure disintegration framework to perform the privacy preservation theme within the cloud. It maintains the load by providing high security within the cloud server. However, it did not utilize cryptologic models effectively.

C. DIFFICULTIES

1. The issues of the Privacy Paradigm are discussed here; • Digital healthcare is gaining growing acceptance in the field to promote the distribution and storing of large data through e-health.

However, maintaining the safety and confidentiality of healthcare data across the network results in the cloud provider getting significant problems [9].

2. Privacy problems, such as device losing access control over patient confidential data, are a big concern of cloud network healthcare IT protection. Since the program does not have patients ' private records, performance and collision tolerance are the issues that render the health system unsafe [10].
3. Maintaining the correct usefulness and protection of cloud-related data faces a difficult challenge in the healthcare system [2].
4. Due to the difficulty of performance, protection and usability, the implementation of a model for privacy conservation utilizing a three-factor protocol remains a complicated issue in the difficult problem [9].

D. STRATEGIC GLOWWORM SWARM-BASED WHALE OPTIMIZATION ALGORITHM FOR CLOUD PRIVACY PROTECTION

To secure patient-sensitive data in cloud setting, cloud security protection frameworks are needed. The work uses the suggested GWOA algorithm to implement privacy protection process for healthcare data in the cloud context the recommended solution to privacy protection in health care data involves the following steps: Initially, patient input data is gathered and submitted to the filtering method to conduct privacy protection phase. The filtering method uses the 2D IIR filter answer filter factoring to produce the filter matrix which is made up of two separate filter coefficients used to construct the privacy preserved data in fact, the protection of medical details is protected utilizing the new GWOA method, which is the convergence of GSO [17], and WOA [18], a method. The resultant data will be processed in the data collection network, where the retained data will be registered the saved medical data is eventually processed in the cloud management network. Hence the computer patient can access the computer environment's privacy-preserved medical details. Figure 1 displays the block diagram for the suggested paradigm of privacy protection focused on GWOA.

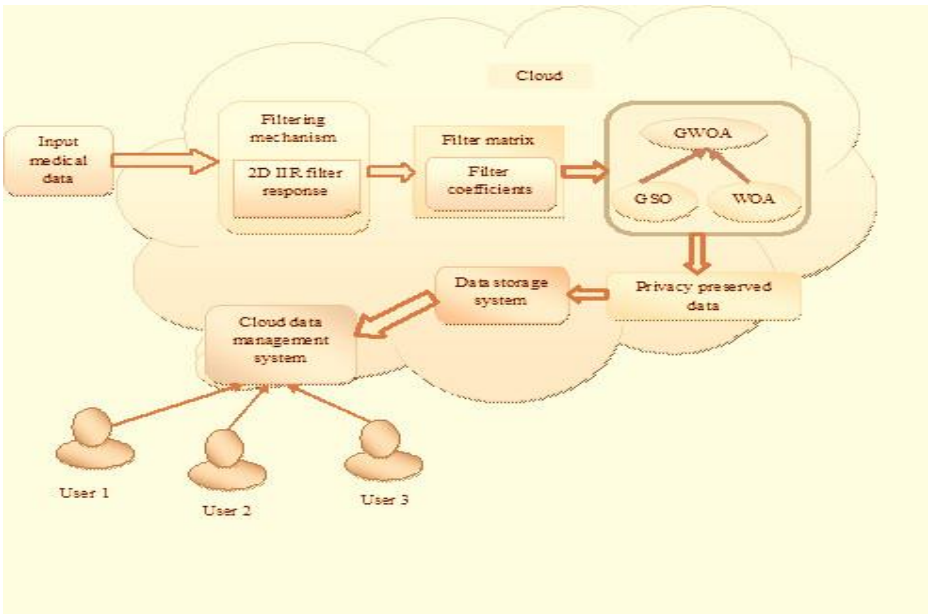

Fig 1: A structure diagram of the current GWOA Privacy Algorithm

- **Input Data of Medical to protect privacy**

Using the suggested GWOA method, input medical data is obtained from the database and the privacy protection framework analyzed for the input data. The planned privacy protection

scheme in the cloud infrastructure safeguards the patient's confidential data. The data held in the cloud system protected for protection is open to the computer customer.

- **Filtering process utilizing 2D IIR filter response**

Collected input data is exposed to the filtering method, where 2D IIR filter response filtering is used to produce a filter matrix. The filter matrix includes the filter coefficient and is often used to conduct the cycle of privacy protection. The corresponding filter matrix computed using the address filter is mathematical.

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

Where, denotes the dimension of $[b \times c]$ the filter matrix, is the index. Above, and below are the filter coefficients f(ma,m2)&g(n1,n2) determined using the GWOA algorithm suggested. In addition, the medical data is encrypted utilizing the encryption method increasing the key and database with a. dimension.

E. GLOWWORM SWARM-BASED WHALE OPTIMIZATION ALGORITHM DESIGNED TO MEASURE FILTER COEFFICIENTS

The optimization algorithm is being used to measure the filter matrix coefficients, as well as the GWOA is the central addition. In the suggested GWOA, the hunting behavior of meta-heuristic optimization and the swarming actions of the glowworms are inherited. Accordingly, GSA and WOA are paired together by combining GSA and WOA parametric functionality to greatly secure the the sensitive data. The filter matrix created by the filtering process by both the medical data contains two different filter coefficients as well as. These filter coefficients are determined using the proposed GWOA algorithm, which is expressed in the solution encoding by means of the fitness measure.

- **Pseudo coding of GWOA algorithm Proposed :**

Sl. No	**Pseudo code of GWOA rule**
1	Population **data formatting** with **range** of glowworms
2	Specify the step size
3	denotes the position **lightning bug** at time
4	deploy the **lightning bug** agents **at random**
5	for $u = 1$ to d
6	do
7	{

8	$h_u(0) = h_0$
9	situate the highest number of iteration as P
10	situate $z = 1$
11	while $z < P$
12	do
13	{
14	work out the luciferin inform phase for each glowworm u using Eq. (17)
15	work out the progress phase for every glowworm u using Eq. (18)
16	work out the glowworm activities using Eq. (19)
17	$z \leftarrow z+1$
18	} }

F. COMPARATIVE DISCUSSION

This segment explains the comparative review of the proposed GWOA algorithm utilizing the criteria, such as anonymity, and usefulness about the percentage of preparation. Table 1 displays the algorithm suggested for the comparative debate. It is found from the above table that the proposed GWOA algorithm obtained stronger privacy and efficiency than 0.2619 and 0.8786 for the Hungarian dataset of 256 main size. Comparative analysis is performed using 3 datasets named Hungarian dataset, Cleveland dataset, and Switzerland dataset. proposed work is compared with GA,WOA,RGADP and BSWOA algorithms.

Table1. Proportional discussion

Dataset	Key size	Metrics/ Methods	GA	WOA	RGADP	BSWOA	Proposed GWOA
Hungarian	***128***	***Privacy***	0.1101	0.1265	0.1449	0.1581	**0.2232**
		Utility	0.6463	0.7385	0.7787	0.7887	**0.8783**
	256	***Privacy***	0.1168	0.1300	0.1457	0.1825	**0.2619**
		Utility	0.6429	0.7384	0.7785	0.7886	**0.8786**
Cleveland	***128***	***Privacy***	0.1511	0.1720	0.1849	0.1924	**0.2462**
		Utility	0.3740	0.7292	0.7692	0.7793	**0.8692**
	256	***Privacy***	0.1053	0.1054	0.1388	0.1653	**0.2873**
		Utility	0.3902	0.7292	0.7693	0.7796	**0.8688**
Switzerland	***128***	***Privacy***	0.1080	0.1142	0.1318	0.1565	**0.2456**
		Utility	0.5314	0.7386	0.7784	0.7884	**0.8784**
	256	***Privacy***	0.1281	0.1481	0.1614	0.1644	**0.2698**
		Utility	0.5347	0.7385	0.7785	0.7884	**0.8786**

G. CONCLUSION

In this study, using the proposed Glowworm Swarm-based Whale Optimization algorithm, the privacy protection method is carried out for healthcare data in the cloud world. The input medical data is initially collected and subjected to the filtering system to conduct the process of privacy conservation. The filtering process is performed using the response of the 2D IIR filter to produce a filter matrix using the model for filter factoring. The filter matrix is used to create data maintained for the privacy. In addition, the privacy of medical data is maintained using the proposed Glowworm Swarm whale optimization algorithm, which is the combination of Glowworm Swarm Optimization and Whale Optimization Algorithm, respectively. The data stored resulting in privacy is subjected to the data storage system, where the stored data is registered. Instead, the retained data is stored in the cloud infrastructure information management system. The proposed Glowworm Swarm Whale Optimization algorithm therefore reported better results using metrics such as privacy and usefulness with values of 0.2698 respectively 0.8786 for 256 key Scale with database of Switzerland. In the future, the privacy protection of medical data will be done and used some certain technique of optimization.

REFERENCES

[1] Alphonsa M.A. and Amudhavalli P, "Genetically modified glowworm swarm optimization based privacy preservation in cloud computing for healthcare sector", Evolutionary Intelligence, vol. 11, no. 1-2, pp.101-116, 2018.

[2] Karlekar N.P. and Gomathi N., "Kronecker product and bat algorithm-based coefficient generation for privacy protection on cloud", International Journal of Modeling, Simulation, and Scientific Computing, vol. 8, no. 03, pp.1750021, 2017.

[3] Tong Li, Zheli Liu, Jin Li, Chunfu Jia and Kuan-Ching Li, "CDPS: A cryptographic data publishing system", Journal of Computer and System Sciences, nol. 89, pp.80-91, 2017.

[4] Li J., Wei J., Liu W and Hu X., "PMDP: A Framework for Preserving Multiparty Data Privacy in Cloud Computing", Security and Communication Networks, 2017.

[5] Piao C., Shi Y., Yan J., Zhang C. and Liu L., "Privacy-preserving governmental data publishing: A fog-computing-based differential privacy approach", Future Generation Computer Systems, vol. 90, pp.158-174, 2019.

[6] Song W., Wang B., Wang Q., Peng Z., Lou W. and Cui Y., "A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications", Journal of Parallel and Distributed Computing, vol. 99, pp.14-27, 2017.

[7] Wu Z., Xu G., Lu C., Chen E., Jiang F. and Li G., "An effective approach for the protection of privacy text data in the CloudDB", World Wide Web, vol. 21, no. 4, pp.915-938, 2018.

[8] Rawal B.S., Vijayakumar V., Manogaran G., Varatharajan R. and Chilamkurti N., "Secure disintegration protocol for privacy preserving cloud storage", Wireless Personal Communications, pp.1-17, 2018.

[9] Jiang Q., Khan M.K., Lu X., Ma J. and He D., "A privacy preserving three-factor authentication protocol for e-Health clouds", The Journal of Supercomputing, vol. 72, no. 10, pp.3826-3849, 2016.

[10] Shrestha N.M., Alsadoon A., Prasad P.W.C., Hourany L. and Elchouemi A., "Enhanced e-health framework for security and privacy in healthcare system", Sixth International Conference in Digital Information Processing and Communications (ICDIPC), IEEE, pp. 75-79, April 2016.

[11] Rahman S.M.M., Masud M.M., Hossain M.A., Alelaiwi A., Hassan M.M. and Alamri,A., "Privacy preserving secure data exchange in mobile P2P cloud healthcare environment", Peer-to-Peer Networking and Applications, vol. 9, no. 5, pp.894-909, 2016.

[12] AL Hamid H.A., Rahman S.M.M., Hossain M.S., Almogren A. and Alamri A., "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography", IEEE Access, vol. 5, pp.22313-22328, 2017.

[13] Zhou J., Cao Z., Dong X. and Lin X., "PPDM: privacy-preserving protocol for dynamic medical text mining and image feature extraction from secure data aggregation in cloud-assisted e-healthcare systems", IEEE, Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp.1332-1344, 2015.

[14] Sreedhar K.C. and Suresh Kumar N., "An optimal cloud-based e-healthcare system using k-centroid MVS clustering scheme", Journal of Intelligent & Fuzzy Systems, vol. 34, no. 3, pp.1595-1607, 2018.

[15] Park J. and Lee D.H., "Privacy Preserving k-Nearest Neighbor for Medical Diagnosis in e-Health Cloud", Journal of healthcare engineering, 2018.

[16] Karlekar N.P. and Gomathi N., "OW-SVM: Ontology and whale optimization- based support vector machine for privacy preserved medical data classification in cloud", International Journal of Communication Systems, p.e3700, 2018.

[17] Kaipa K.N. and Ghose D., "Glowworm Swarm Optimization: Algorithm Development", In Glowworm Swarm Optimization, pp. 21-56, Springer, Cham, 2017.

[18] Mirjalili S. and Lewis A., "The whale optimization algorithm", Advances in Engineering Software, 95, pp.51-67, 2016.

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

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

[21] Lu, R., Liang, X., Li, X., Lin, X. and Shen, X., "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, 2012.

[22] [Pan, Y. Xiaolin, G. Jian, A. Jing, Y. Jiancai L. and Feng, T. "A Retrievable Data Perturbation Method Used in Privacy-Preserving in Cloud Computing, China communications, vol. 11, pp. 73-84, 2014.

[23] Keshanchia, B. Souria, A. and Navimipourb, N.J. "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, 2017.

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