DISCRETE AND CONTINUOUS
DYNAMICAL SYSTEMS SERIES S
Volume **12**, Number **4&5**, August & September **2019**

doi:10.3934/dcdss.2019084

pp. **1219–1232**

REVERSIBLE HIDDEN DATA ACCESS ALGORITHM IN CLOUD COMPUTING ENVIRONMENT

Jinsong Xu*

School of Modern Posts & Institute of Modern Posts
Nanjing University of Posts and Telecommunications
Nanjing 210003, China

Abstract. At present, the data filtering quality of reversible hidden data access algorithm based on column store database is not guaranteed, and the location accuracy and data access security of reversible hidden data are low. In this paper, the whitening vector is obtained by processing the sample length of the observed data signal. By using the nonlinear robust function, the data projection is realized, the judged threshold of projection data is constructed, an matrix with adaptive filter characteristic is set up, and the high quality of filtering results are output; the parameters between three anchor nodes and the location of reversible hidden data are measured, and the artificial bee colony optimization neural network is used for modeling and forecasting the ranging error, and determine the weights according to the results, so that on the basis of the three edge location algorithm, the positioning accuracy of the data is to further improve;through the establishment of authorized institutions, producing key, off-line encryption, online encryption, ciphertext conversion, decrypt ion and other aspects, the security of access data is completed. The experiment shows that the algorithm can effectively improve the quality of data filtering and positioning accuracy and the security of data access is also better than that of the current algorithm.

1. **Introduction.** The rapid development of network technology and the large number of applications of information sharing system provide a lot of value-added services based on network information transmission and access. However, while users enjoy the convenience of service, the risk of reversible data access leakage in the database is also increased [18, 21]. To this end, countries such as the United States and other countries have issued a specification for access control of data privacy information, such as HIPAA and DECD.

In order to integrate privacy controls standard of these reversible hidden data in a database, while also taking into account the limitations of the existing database access control technology in the face of open environment, dynamic application scenarios and the data access control the under emergency situation, Hippocratic Database proposes access control technology based on data access to data privacy, it is a database management system which allows a reasonable use of data privacy information and reasonable leakage [8, 14]. For the cloud computing environment, the reversible hidden data is of great value, and its access research is the development focus of data control area [12].

2010 *Mathematics Subject Classification.* 05C57.
Key words and phrases. Cloud computing environment, reversible hidden data, access.
* Corresponding author: Jinsong Xu.

With the expansion of data and information in cloud computing environment, the development of database technology is changing rapidly. The database has evolved from the traditional single database and LAN database to the current Web database. The database scale is developing towards cluster and cascade [9,13]. The deep, secure and accurate access of network concatenated database has become a hot topic in the field of computer network and data processing, widely concerned by many scholars [15,22]. In the traditional algorithm, the algorithm for accessing reversible hidden data in a network cascaded database is mainly divided into histogram translation and feature recovery filtering. The histogram translation method has the advantages of simple implementation and small computation, but the access performance is poor, and the accuracy of the reversible hidden data location is low.

In view of the above problems, a high efficient reversible hidden data access algorithm is proposed to achieve accurate location and access of reversible hidden data in the database.

2. Reversible hidden data access algorithm in cloud computing environment.

2.1. Reversible hidden data filtering.

In reversible hidden data filtering, it is necessary to establish a dynamic decision method based on the data itself because of the inability to obtain the prior knowledge of the data [6,7]. In this paper, the nonlinear projection of observed data is used as a part of decision. Based on that, the mean square value of nonlinear projection is constructed as the judgement basis of adaptive thresholds, which can be expressed as:

$$Q = \sqrt{\frac{1}{l}\sum_{i=1}^{l}\left(F\left(z,w\right)\right)^2} \tag{1}$$

Where, l represents the length of the data sample, $F(z,w)$ represents a robust nonlinear projection, and i represents the number of data. According to the formula (1), it is easy to find that the threshold changes dynamically with the nonlinear projection of the observed data. From the characteristics of statistics, it can be seen that the mean square value of the nonlinear projection reflects the relative effective value of data, which has important reference for statistical analysis of reversible hiding data.Due to the existence of magnitude and positive and negative uncertainties in reversible hidden data, the mean square value of nonlinear projection eliminates the influence of symbols. It can be used as a discrete reference for reversible hidden data, which is reflected in data statistics.

To sum up, a $l*l$ dimensional adaptive filter with dynamic performance can be constructed, which can be expressed as:

$$M_{l*l} = \begin{bmatrix} \ldots & 1 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 1 & 1/2 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0_k & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 1/2 & 1 & 0 & \ldots \end{bmatrix} \tag{2}$$

Where, k represents the filter coefficient.

Obviously, for the formula (2), the mechanism of its filtering is that x_{ik} and $i = 1, 2, \ldots, k$, which are judged as a reversible hidden data component replaced by the arithmetic mean value of the two data. If the reversible hidden data component appears at the boundary point (beginning and ending), the mean value of the

adjacent data points can be used to instead [17]. Using this algorithm to filter the observed data of reversible hidden data, it can maintain the statistical characteristics of the data as much as possible, and solve the drawback of low pass or high pass filter. In reversible hidden data processing, it is impossible to determine the order of source signals in mixed data, so it is necessary to establish a conservative and reliable filter. Specifically, it can be expressed as:

$$Y = X * M \tag{3}$$

An adaptive filtering algorithm for reversible hidden data signals can be obtained according to the formula (3).

(1) The sample length of the observation signal X is l, it is centralized and formula (4) is applied to the spheralization of the sample, to obtained the whitening vector z.

$$z = Vx \tag{4}$$

Where, V represents the whitening matrix and x represents the observation data.

(2) the projection of data is realized by the nonlinear robustness function based on formula (5) and formula (6).

$$g_1(\xi) = \begin{cases} a\xi, & \xi \le Q \\ aQ, & \xi > Q \end{cases} \tag{5}$$

$$g_2(\xi) = Q \tan\left(\frac{\xi}{b}\right) \tag{6}$$

Where, $\xi = wz, a$, and b are constant. According to experience, $0 \le a \le 4$, $1 \le b \le 2$.

(3) The decision threshold of the projection data is constructed.

(4) According to the result of the threshold construction, a $l*l$ dimensional matrix M with adaptive filtering characteristics is formed.

(5) The filter results can be output.

2.2. **Reversible hidden data location in cloud computing environment.** According to the filtering results of Section 2.1, the location algorithm is used to locate the reversible hidden data, which lays the foundation for the data access. The whole process can be summarized as follows: the parameters between the three anchor nodes and localization of the reversible hiding the data aremeasured firstly, and then the artificial bee colony optimization neural network is used for modeling and forecasting the ranging error, to determine the weight according to the results. Finally, on the basis of the three edge location algorithm, the location accuracy isto improve. The principle of reversible hidden data location can be expressed in Figure 1.

Figure 1 shows that in general, if it can get to the point to be located and three anchor nodes' information, it can estimate the target position, namely three edge location algorithm, and the basic idea is: the location of the three anchor nodes is as the center of the circle to construct the triangle. Then the distance between the anchor nodes and the location points is as the radius of the circle, so the intersection point of the circle can be regarded as the location to be estimated [2,4,5,10,11], as shown in Figure 2.

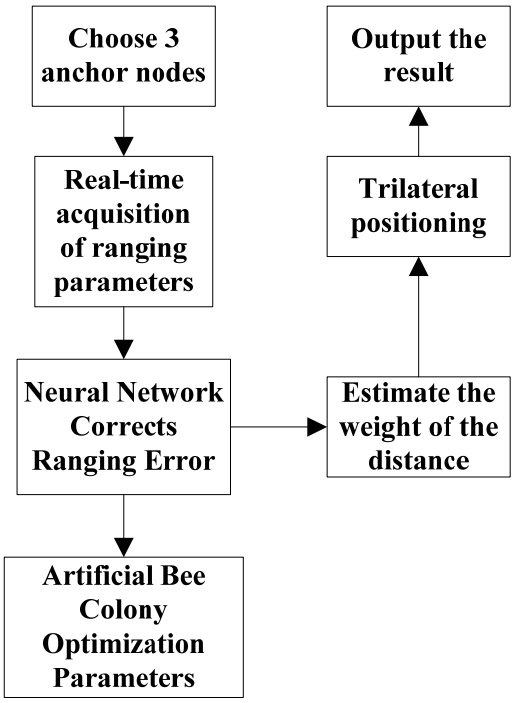


FIGURE 1. principle of reversible hidden data location

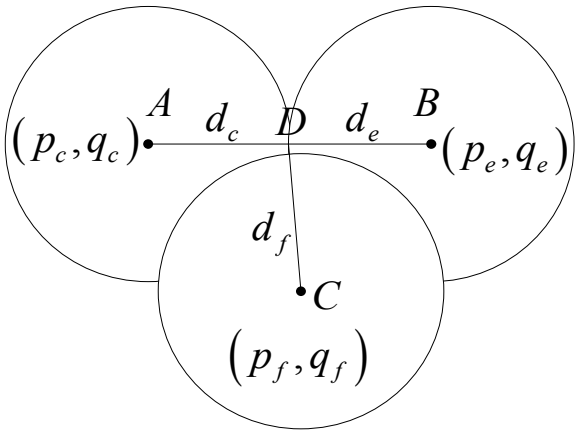


FIGURE 2. working principle of three edge location method

In Figure 2, the location of data point D is (p, q), the locations of three anchor nodes of A, B and C are $(p_A, q_A), (p_B, q_B), (p_C, q_C)$ and the distances between them and D is d_A, d_B and d_C. The following expression can be obtained:

$$\begin{cases} d_A^2 = (p_A - p)^2 + (q_A - q)^2 \\ d_B^2 = (p_B - p)^2 + (q_B - q)^2 \\ d_C^2 = (p_C - p)^2 + (q_C - q)^2 \end{cases} \tag{7}$$

Assuming that the propagation dissipation coefficient of the path is n,and then the formula for receiving the intensity of reversible hidden data signal under normal condition is as follows:

$$RSSI_r = -(10n \lg d + S) \tag{8}$$

Where, S represents the ideal value of $RSSI$.

The change of the formula (8) can be obtained:

$$d = 10^{\frac{(-RSSI_r - S)}{10n}} \tag{9}$$

In practical applications, the values of S and n are not fixed, and are closely related to their environment. At present, the value is determined by some experts based on experience, which leads to a large error of positioning for reversible hidden data [19]. In order to improve the positioning accuracy of reversible hidden data location, the parameter values of S and n are estimated in real time. The signal intensity between the point C of the anchor node and the anchor node A and B is $RSSI_A$ and $RSSI_B$, then the formula is:

$$\begin{cases} RSSI_A = -(10n \lg d_A + A) \\ RSSI_B = -(10n \lg d_B + A) \end{cases} \tag{10}$$

Where, d_A and d_B are Euclidean distances, which can be expressed as:

$$\begin{cases} d_A = \sqrt{(p_C - p_A)^2 + (q_C - q_A)^2} \\ d_B = \sqrt{(p_C - p_B)^2 + (q_C - q_B)^2} \end{cases} \tag{11}$$

The value of S and n is estimated on the basis of the formula (11), which accurately describes the environment state in which the reversible hidden data point is located.

For the determination of weights, relevant research results show that with the increase of the propagation distance of signals, the estimation error of the received signal's strength is also increased, so in the value estimation of parameter S and n, it should also make appropriate adjustments to the distance that is operated by weighting on them, so as to reduce the pitch error [16]. Weight can describe the role of anchor nodes to the nodes to be located. Distance is mainly used to describe the location between nodes to be located and anchor nodes. The weight ω is defined as:

$$\omega = \frac{d_4^2}{\sum d_j^2} \tag{12}$$

Where, d_j represents a sequence of the distance between the reversible hidden data node to be located and the anchor node.

The results of locating reversible hidden data nodes are as follows:

$$(p, q) = \sum_{j=1}^{3} \omega (p_j, q_j) \tag{13}$$

For the correction of ranging error, there may be a certain range error ΔE in the actual operation process. The relationship between the actual distance d and the measurement distance d' is:

$$d = d' + \Delta E \tag{14}$$

In this paper, neural network is used to predict the ranging error, then the ranging error is corrected, and the artificial bee colony algorithm is used to optimize the neural network parameters.

According to the formula (9), the distance error estimation function of reversible hidden data nodes in cloud computing environment is established, and the prediction error is $(\Delta E')$. Thus, the location error correction function of reversible hidden data nodes is as:

$$d'' = d' + (\Delta E') \tag{15}$$

When using neural network to predict the ranging error, the prediction accuracy of the direct measured ranging error can be determined by connecting weights and thresholds. Then, the artificial bee colony algorithm is selected for to optimizing their, in order to better to correct the ranging error to find the weights and thresholds. The steps of neural network on the ranging error prediction are as:

(1) the measurement sequence is collected and the normalization operation is carried out specifically as:

$$\widehat{q}_j = \frac{q_i - q_{\max}}{q_{\max} - q_{\min}} \tag{16}$$

Where, $q_{\max}$ and $q_{\min}$ represent the maximum and minimum values of the vertical coordinates of the reversible hidden data nodes.

(2) The parameters are initialized, including the number of food sources, the number of iterations, the control parameters and the limited interval of the solution.

(3) the location of the food source is initialized:

$$P_j = [p_{j1}, p_{j2}, \ldots, p_{jG}] \tag{17}$$

Where, G represents the data dimension, and the method of determining the dimension is as follows:

$$G = m * H + H * N + H + N \tag{18}$$

Where, m, H, and N represent the number of nodes in the input layer, the hidden layer and the output layer.

(4) according to the position of P_j, the weights and thresholds of the neural network are valued, and the training samples are studied, to obtain the target function of P_j as follows:

$$fit = \frac{1}{n} \sum_{j=1}^{K} \sum_{K=1}^{m} (d_j - t_K)^2 \tag{19}$$

Where, t_K represents the expected output value, and K represents the number of training sample.

(5) The leading bee generates the new solution V_j around P_j, and computes their fitness values. Based on the greedy principle, it is determined to retain the fitness value of 3 and 4 which one is the best.

(6) the solution is chosen according to the selection probability, the new solution V_j is generated around P_j, and the optimal solution is retained in the same way.

(7) supposing that after a number of cycles, a solution is not improved, and the solution is discarded. At this time, the leading bee will be transformed into a spy bee, creating a new solution V_j to instead of the solution.

(8) the optimal solution is found according to the fitness value.
(9) after the termination condition is reached, the optimal weight and threshold value of the neural network are obtained according to the optimal solution, otherwise, it will return (5).
(10) the training samples are relearned according to the optimal weights and thresholds, and the ranging error prediction model is established.
(11) it is corrected according to the result of error prediction.

2.3. **Encrypted access of reversible hidden data in cloud computing environment.** The filtering results and the location results of reversible hidden data in Section 2.1 are as the basis, an efficient access control scheme of reversible hidden data in cloud computing environment consists of four entities: the Data Owner, Cloud Storage Server (CS), a plurality of Attribute Authorities (AAs) and Data User, as shown in figure 3:

In this module, an efficient encryption access scheme of multi-authorized agencies attribute based is concretely constructed in this article. The specific process of access is as follows:

(1) Initialization of the algorithm. Which produces an open parameter $Params$ for data access. A bilinear group is constructed to satisfy $L * L \to L_T$, then data $h, u, v, w \in L$ can be randomly selected, and collision resistant hash function $H(\cdot) : \{0,1\} \to Z_o$ as well as the secure key extraction function H' are constructed, where o represents a prime number and Z_o represents the finite field consisted by o. In addition, it is assumed that there are U attribute authorization mechanisms $\{\widehat{I}_1, \widehat{I}_2, \ldots, \widehat{I}_U\}$ in the algorithm, and each attribute authorized agency manages a class of reversible hidden data attribute sets $\tilde{I}_i = \{I_{i,1}, I_{i,2}, \ldots, I_{i,oi}\}$, of which

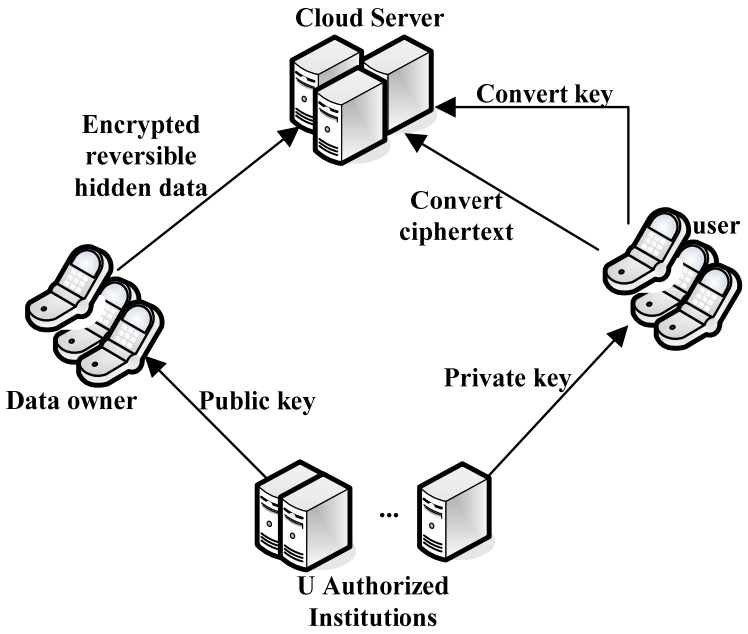


FIGURE 3. reversible hidden data's access control entities in the cloud computing environment

$I_{i,j} \in Z_o$. In the algorithm, the reversible hidden data is transmitted in a secure channel. Thus, the open parameters of the reversible hidden data access system are as follows:

$$Params = (h, u, v, w, H, Z_o, H') \tag{20}$$

(2) the establishment of an authorized institution is divided into the following two steps:

All authorized agencies randomly select $\alpha \in Z_o$ and $y_i = (h, h)^{\alpha}$, and then send y_i to other authorized agencies, and each last authority calculates y independently. For the components g^s of $U - 1$ 6 in each authorized agency $\widehat{A}_i$, the main private key MK_i is calculated by the following formula:

$$MK_i = \frac{\left(\prod_{\widehat{A}_i} g^s\right)}{g^s} \tag{21}$$

According to the formula (21), the authorized agencies publish their own public key PK_i and retain their own private key SK_i.

(3) Private key generation. When new users access reversible hidden data, they need to request private key from the attribute agency. The authorized agency releases the private key for the user by executing the key [24, 26].

(4) off-line encryption. when the data owner's mobile device is restarted, the temporary ciphertext is generated, and the temporary cipher is stored in the mobile device.

(5) online encryption. When the data is outsourced to the cloud storage server by the reversible hidden data owner, it needs to encrypt the data, and then the ciphertext is outsourced to the cloud storage server. The process is as follows:

1. Data owner randomly selects the key, and calculates the symmetric key $sk = H'(ck)$, to encrypts the data with the symmetric key, and generate the data ciphertext CT', and the authentication token $Token$.

2. Data owner encrypts the symmetric key ck.

(6) Ciphertext conversion. when data users start in cloud computing environment, the conversion key is generated and it is stored on mobile devices. The generation process of conversion key is as: firstly, conversion coefficient μ is selected randomly, to get the conversion key. When data users access reversible hidden data, the conversion key is outsourced to the cloud storage server, and the cloud server generates conversion ciphertext TD.

(7) Decryption. After the data users received the converted ciphertext from cloud storage server, the cipher text is decrypted and the process is as follows: firstly, the symmetric key ck is calculated, and then whether $Token \neq (ck)/CT'$ is established is to verify. If is is true, the decryption of cloud storage server is incorrect; if it is false, it means that the decryption of cloud storage server is correct, and then the symmetric key ck is used to decrypt CT' and return the plaintext, to realize the complete the secure access of reversible hidden data. It is characterized by the security factor to judge whether the reversible hidden data access is secure. The closer the security factor is to 1, the more secure the data access algorithm represents [1, 3, 20, 23, 25]. Whether the security of the algorithm proposed in this paper can meet the requirement of reversible hidden data access, it is given in the experiment.

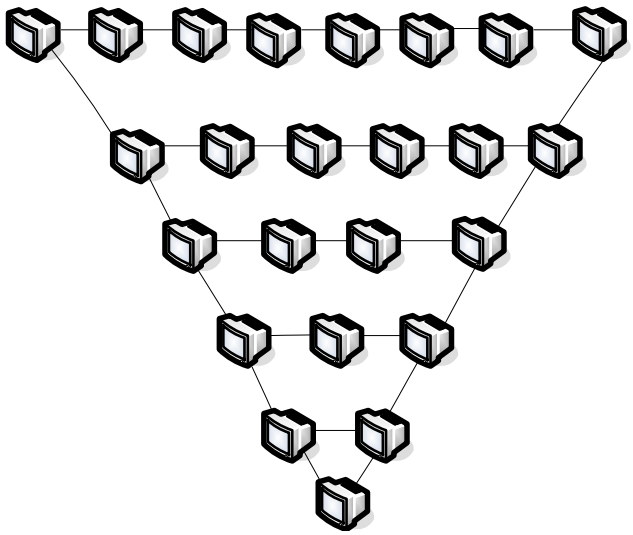


FIGURE 4. Distribution model of reversible hidden data node in cloud computing environment

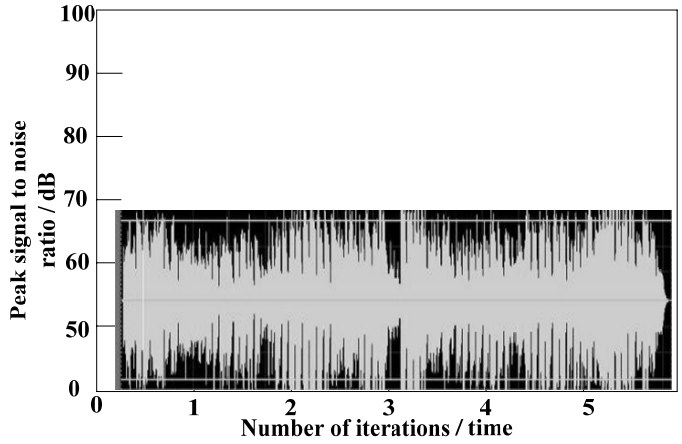
3. **Experimental results and analysis.** In this paper, the experimental platform is built on MATLAB, and the large concatenated database K2CH is taken as the research sample. Through setting up 24 network node machines, the database is simulated to distribute in different network nodes to complete the experiment. The model is shown in Figure 4. To access the time series with target length of 120000, the proposed access algorithm is used to build database and reversible hidden data signal model, and verify the algorithm in the following aspects.

(1) the overall effect of the algorithm on the data filtering;
(2) the location accuracy reversible hidden data;
(3) the security of hidden reversible data access.

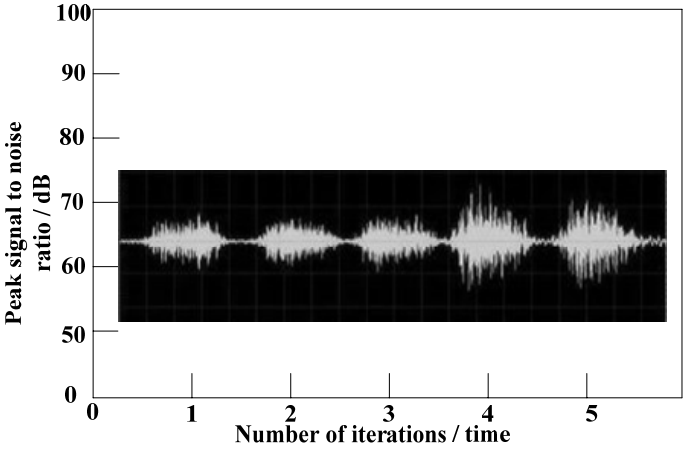
The results of the experiment are as follows:

The experimental results of Figure 5 are analyzed. The unfiltered data has many burrs and large fluctuation. After filtering by the current algorithm, the filtering effect has played a significant role, but the running band of data is not very stable. In this paper, the proposed algorithm is used to filter the data operation waveform, the projection by nonlinear robust function is realized, to construct the judgment threshold of projection data. According to the construction results of threshold, a matrix with the characteristics of adaptive filtering can be established, and the filtering result and other steps are output to realize the efficient data filtering. And using this algorithm, the data signal observation data of reversible hidden data can be filtered, which can maximum keep the statistical properties of the data from the whole, and solve the low-pass or high pass filter shortcomings, making that the proposed algorithm has superiority compared with the current algorithm.

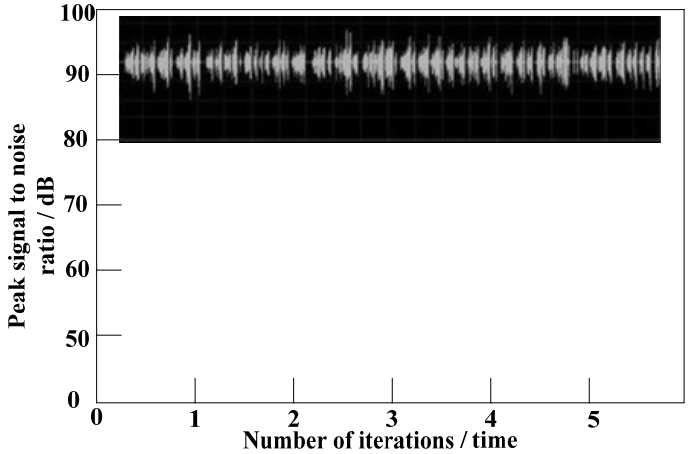
In Figure 6, they represent a number of rows, several rows of arranged reversible hidden data, and interfering data. Among them, the square data represents the reversible hidden data, and the other represents the interference data, in order to observe the location effect of the different algorithms on the reversible hidden data. The experimental results are as follows:



(a) the operation waveform of the data before filtering

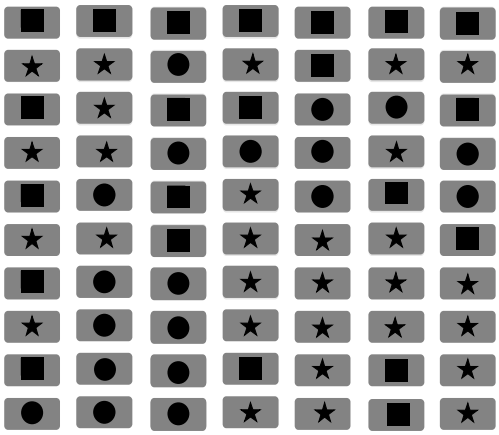


(b) the filtering effect of the current algorithm

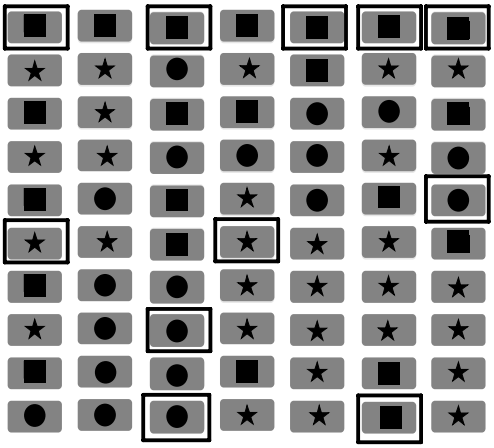


(c) the filtering effect of the proposed algorithm

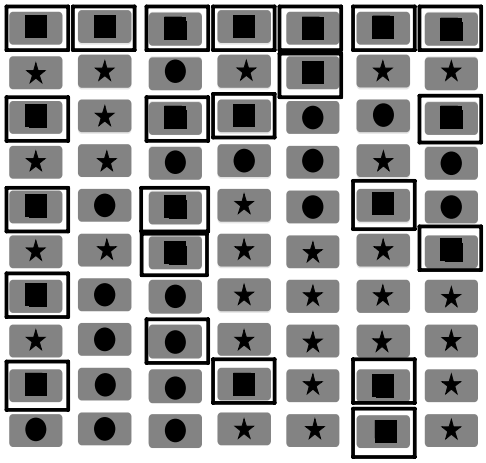
FIGURE 5. Comparison of the filtering effects by different algorithms



(a) the location effect of reversible hidden data by the experimental model



(b) the location effect of reversible hidden data by the current algorithm

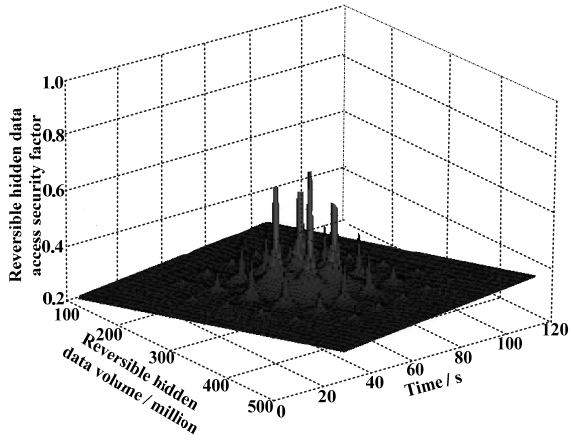


(c) the location effect of reversible data hidden by the proposed algorithm

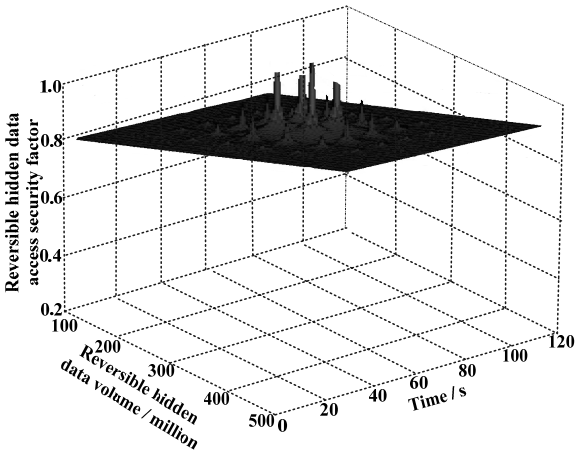
FIGURE 6. Comparison of location effect of reversible hidden data by different algorithms

As shown in Figure 6, the algorithm proposed in this paper is more accurate in locating reversible hidden data than that of the current algorithm. In the proposed algorithm, three anchor nodes are measured and parameters between the reversible hidden data are located, and then artificial bee colony optimization neural network is used for modeling and forecasting the ranging error, to determine the weights according to the detection results. Finally, on the basis of the three edge location algorithm, it is to further improve the location accuracy. Among them, when using neural network to predict the ranging error, the prediction accuracy of the direct ranging error is determined by connecting weights and thresholds, and the artificial bee colony algorithm is used for their optimization, to correct the ranging error better and find the weights and thresholds. This link can greatly enhance the location effect of reversible hidden data by the proposed algorithm.

Through the experimental results of Figure 7, it is observed that the access security coefficient of reversible hidden data by using the propose algorithm is much higher than that of the current algorithm. The proposed algorithm uses the filtering



(a) the access security of reversible hidden data by the current algorithm



(b) the access security of reversible hidden data by the proposed algorithm

FIGURE 7. Comparison of access security for reversible hidden data by different algorithms

result and reversible hidden data as basis, and put forward efficient access control scheme for reversible hidden data in cloud computing environment which consists of four entities: the Data Owner, Cloud Storage Server (CS), a plurality of Attribute Authorities(AAs) and Data User, to respectively establish the authorized agency and generate private key. When new users visit reversible hidden data, the property authorities request the private key and through the implementation of key, the authorities publish the private key and make offline encryption for users. When the mobile device of data owner restarts, a temporary ciphertext is generated, and the temporary ciphertext is stored in mobile devices, then the process of online encryption, ciphertext conversion and decryption conversion are carried out to complete the secure access of reversible hidden data, making the overall safety performance of the proposed algorithm is higher than that of the current algorithm.

4. **Conclusions.** Under the cloud computing environment, reversible hidden data access is a current research hotspot. Among them, access control is a technology that almost all systems need to used, including computer systems and non computer systems. Access control is giving a set of strategies to identify all the functions in the system, organize it and host it, then providing a simple and unique interface. One end of the interface is at the end of the application system, is the permission engine. The permission engine answers only who has the authority to carry out a certain action (motion, calculation) to a resource. The result of the return is only yes, no or that the privilege engine is abnormal. Aiming at the complexity of reversible hidden data access in cloud computing environment, this paper proposes using data filtering, reversible hidden data location and data encryption access to achieve secure access and control of data, and experiments prove that the algorithm is reliable.

REFERENCES

[1] R. Afshari, B. S. Gildeh and M. Sarmad, Fuzzy multiple deferred state attribute sampling plan in the presence of inspection errors, *Journal of Intelligent & Fuzzy Systems*, **33** (2017), 503–514.

[2] A. Bahl, S. Masson, Z. Malik, A. J. Birtle, S. Sundar, R. J. Jones, N. D. James, M. D. Mason, S. Kumar and D. Bottomley, Final quality of life and safety data for patients with metastatic castration-resistant prostate cancer treated with cabazitaxel in the uk early access programme (eap) (nct01254279), *Bju International*, **116** (2015), 880–887.

[3] A. Basar and M. Abbasi, On ordered bi–ideals in ordered-semigroups, *Journal of Discrete Mathematical Sciences and Cryptography*, **20** (2017), 645–652.

[4] J. Bensmail and B. Stevens, Edge-partitioning graphs into regular and locally irregular components, *Discrete Mathematics*, **17** (2016), 43–58.

[5] A. Brezavscek, S. P. and Z. A., Factors influencing the behavioural intention to use statistical software: The perspective of the slovenian students of social sciences, *Eurasia Journal of Mathematics Science and Technology Education*, **13** (2017), 953–986.

[6] K. Caine, S. Kohn, C. Lawrence, R. Hanania, E. M. Meslin and W. M. Tierney, Designing a patient-centered user interface for access decisions about ehr data: Implications from patient interviews., *Journal of General Internal Medicine*, **30** (2015), 7–16.

[7] K. Caine and W. M. Tierney, Point and counterpoint: Patient control of access to data in their electronic health records, *Journal of General Internal Medicine*, **30** (2015), 38–41.

[8] T. H. Chen, W. Shang, Z. M. Jiang, A. E. Hassan, M. Nasser and P. Flora, Finding and evaluating the performance impact of redundant data access for applications that are developed using object-relational mapping frameworks, *IEEE Transactions on Software Engineering*, **42** (2016), 1148–1161.

[9] P. K. Commean, J. M. Rathmell, K. W. Clark, D. R. Maffitt and F. W. Prior, A query tool for investigator access to the data and images of the national lung screening trial, *Journal of Digital Imaging*, **28** (2015), 439–447.

[10] J. Dou, Z. Zhang, J. Dang, L. Wu, Y. Wei and C. Sun, Properties and achievable data rate of a cyclic prefix based imperfect reconstruction filter bank multiple access system, *Iet Communications*, **10** (2016), 2427–2434.
[11] W. Gao and W. Wang, A tight neighborhood union condition on fractional (g, f, n', m)–critical deleted graphs, *Colloquium Mathematicum*, **149** (2017), 291–298.
[12] P. Gope and T. Hwang, A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks, *IEEE Transactions on Industrial Electronics*, **63** (2016), 7124–7132.
[13] F. Guo and T. Cheng, Systems and methods for detecting suspicious attempts to access data based on organizational relationships, 2015.
[14] D. Huang, D. Han, J. Wang, J. Yin, X. Chen, X. Zhang, J. Zhou and M. Ye, Achieving load balance for parallel data access on distributed file systems, *IEEE Transactions on Computers*, **67** (2018), 388–402.
[15] M. Kumar, N. P. Gantasala, T. Roychowdhury, P. K. Thakur, P. Banakar, R. N. Shukla, M. G. Jones and U. Rao, De novo transcriptome sequencing and analysis of the cereal cyst nematode, heterodera avenae, *Plant Molecular Biology*, **1** (2015), 69–80.
[16] Y. Kwon, B. Park and D. H. Kang, Scaling of data retention statistics in phase-change random access memory, *IEEE Electron Device Letters*, **36** (2015), 454–456.
[17] O. Lancaster, T. Beck, D. Atlan, M. Swertz, D. Thangavelu, C. Veal, R. Dalgleish and A. J. Brookes, Cafe variome: General-purpose software for making genotype–phenotype data discoverable in restricted or open access contexts, *Human Mutation*, **36** (2015), 957–964.
[18] F. Li, B. Liu and J. Hong, An efficient signcryption for data access control in cloud computing, *Computing*, **99** (2017), 465–479.
[19] T. L. Spires-Jones, P. Poirazi and M. S. Grubb, Opening up: open access publishing, data sharing, and how they can influence your neuroscience career, *European Journal of Neuroscience*, **43** (2016), 1413–1419.
[20] L. Y. Wang, L. Chen, X. R. Hao, Q. Wang and M. Ni, Life-aware buffer management algorithm for flash-based databases, *Jilin Daxue Xuebao*, **47** (2017), 632–638.
[21] Z. Wang, D. Huang, Y. Zhu, B. Li and C. J. Chung, Efficient attribute-based comparable data access control, *IEEE Transactions on Computers*, **64** (2015), 3430–3443.
[22] D. T. Wiriaatmadja and K. W. Choi, Hybrid random access and data transmission protocol for machine-to-machine communications in cellular networks, *IEEE Transactions on Wireless Communications*, **14** (2015), 33–46.
[23] F. Y. Wu, Remote sensing image processing based on multi-scale geometric transformation algorithm, *Journal of Discrete Mathematical Sciences & Cryptography*, **20** (2017), 309–321.
[24] J. Xu, Data distributed momdatory secure access method in cloud computing environment, *Bulletin of Science & Technology*, **8** (2017), 189–192.
[25] T. Yin, The exploration and research of software development architecture based on asp.net mvc pattern, *Journal of China Academy of Electronics & Information Technology*, 599–602.
[26] J. Zhang, Simulation of database access information security management under big data platform, *Computer Simulation*, **7**.

Received June 2017; revised November 2017.

E-mail address: xujs@njupt.edu.cn