Research on a New Attribute Encryption Anonymous Algorithm in Cloud Computing Environment

Xin Zha*

Zibo Vocational Institute, Zibo, 255000, Shandong Province, China
*Corresponding Author Email: 11484@zbvc.edu.cn

Abstract. The attribute encryption anonymous model is used to encrypt data and protect anonymity in cloud computing environment, so as to realize attribute encryption and privacy protection in cloud computing environment. In order to improve the self-adaptability and accurate control of data encryption in cloud computing environment, an anonymous data encryption algorithm based on hyperbolic cyclic mapping is proposed. The priority list control model of adaptive privacy protection for cloud data is constructed. The load balancing control and encryption key design of anonymous big data with hyperbolic cyclic mapping are implemented by using bilinear differential control protocol. The hyperbolic differential equation control and adaptive weighting method are used to construct the key function for anonymous encryption of cloud computing data. The time window and privacy protection protocol of attribute encryption anonymous control is optimized by slot allocation. The encryption anonymous algorithm is improved. Simulation results show that the adaptive equalization performance of attribute anonymous encryption in cloud computing environment is better, the ability of anti-attack is better, and the recall rate of data is better than the traditional method.

1. Introduction

With the development of database and network technology, people's network activities become more and more active. People pay more attention to the protection of network privacy information. A large number of personal data are stored in the network system through cloud storage and distributed network database[1]. It is necessary to integrate and analyze big data digitally. Many data holders remove identification fields and publish micro data. In order to prevent the disclosure of personal privacy, the anonymous encryption model of anonymous cloud computing data based on hyperbolic cycle mapping is constructed by means of attribute encryption and anonymous control. It is very important to study the data encryption algorithm of hyperbolic loop mapping anonymous cloud computing environment in order to improve the attribute encryption and privacy protection of network users, the related algorithms have been paid great attention[2].

In recent years, the research of anonymous encryption algorithm for cloud computing data is mainly to implement k-anonymous processing by generalization and suppression. The main scheduling models include energy balanced scheduling model, priority list diversity distributed scheduling model, load balancing scheduling model, hyperbolic loop mapping based on neural network control, anonymous cloud computing data anonymous encryption model and so on. The above methods construct the loop stack control information list of big data time series. The method of data and information fusion is used to design task allocation and load balance, and good scheduling effect is achieved[3]. Wherein, reference [4] uses the generalized control method in binary search domain to encrypt data and protect anonymity in cloud computing environment, so that network data intruder cannot distinguish the attribute and category of privacy information. The privacy leakage can
be avoided effectively and the anonymous scheduling performance of data can be improved. However, the model has delay in the representation of sensitive attributes of data scheduling, and the computational overhead is high. In reference [5], a best k-anonymous NP-hard scheduling model based on hashing technique is proposed. By using K-means clustering analysis of the initial microscopic data table of big data, the classification and scheduling ability of big data is improved. However, the scheduling performance of this scheduling method is poor under the influence of large information feature interference[6].

In order to improve the self-adaptability and accurate control of data encryption in cloud computing environment, an anonymous data encryption optimization algorithm based on hyperbolic loop mapping in cloud computing environment is proposed. The priority list control model of adaptive privacy protection for cloud data is constructed. The load balancing control and encryption key design of anonymous big data with hyperbolic cyclic mapping are implemented by using bilinear differential control protocol. The key function of anonymous encryption of cloud computing data is constructed with adaptive weighted control method. The time window and privacy protection protocol of attribute encryption anonymous control is optimized by slot allocation. Implementation of encryption anonymous algorithm to improve the design. Finally, the performance test is carried out through the simulation experiment, which shows the superiority of this method in improving the anonymous encryption performance of anonymous cloud computing data of hyperbolic cyclic mapping, and the effective conclusion is obtained.

2. Priority List Control Model for Data Encryption in Cloud Computing Environment

2.1. Construction of Anonymous Encryption Mechanism for Anonymous Cloud Computing Data Using Hyperbolic Cyclic Mapping

In order to improve the performance of anonymous scheduling of hyperbolic cyclic mapping in big data environment, the anonymous encryption optimization algorithm for anonymous cloud computing data of hyperbolic cyclic mapping is studied[7]. The priority list of data encryption in cloud computing environment is controlled by feature extraction. Attribute anonymous encryption in cloud computing environment mainly uses vertical and tree network structure for slot control, as shown in figure 1.

![Mesh structure model of attribute anonymous encryption in cloud computing environment](image)

(a) Longitudinal mesh  (b) Tree mesh

Figure 1. Mesh structure model of attribute anonymous encryption in cloud computing environment

In the above cloud computing data anonymous encryption grid model, the hyperbolic loop mapping anonymous cloud computing data anonymous encryption clustering mechanism is designed, and the binary directed graph $G = (V,E)$ is used to represent the clustering nodes of data encryption in cloud computing environment. The time series of information resource allocation in large database are $\{x(t_i + \Delta t)\}$, $i = 0,1, \ldots, N-1$. The real-time task control of data encryption in k-anonymous cloud computing environment is carried out by link recombination, and the clustering time series $\{x(t_i + \Delta t)\}$, $i = 0,1, \ldots, N-1$ are obtained, and the scheduling in the domain of state space information is obtained[8]. The network layer of service is $l(n)$ layer, and the number of hops is $\text{hop\_count}$. The anonymous big data of hyperbolic cyclic mapping is partitioned sequentially according to the feature matching degree. The transmission channel between the $l(n)$ link layer and sink in the open network
large database is $\overline{D_{(\omega)}}$. The scheduling information flow in the state space of the data structure is obtained as follows:

$$flow_q = [n_1, n_2, \ldots, n_q], q \in N \quad (1)$$

In the above formula, $q$ represents the difference characteristic function on the cluster head node, $n_q$ represents the transmission unit data sequence of anonymous data set resources, and $N$ represents the total number of scheduling tasks[9]. Based on the k-anonymous protection model, the variance of the relative difference of scheduling task latency in big data environments is expressed as:

$$\text{Var}(R(q)) = \frac{1}{m^2} \sum_{i=1}^{m} \left( \frac{1}{\sqrt{\text{sup}_{j}(q \Theta q)_{j}}} \left( \frac{(P(q_i) - P(q_j))}{\sqrt{\text{sup}_{j}(q \Theta q)_{j}} - \sqrt{\text{sup}_{j}(q \Theta q)_{j}}} \right) \right) \quad (2)$$

In the formula, $\text{Var}(R(q))$ and $|q|$ show a linear relationship, which increases with the increase of data attribute value combination $|q|$.

Assuming that the anonymous big data adaptive delay difference characteristic $q$ and $q'$ of hyperbolic cyclic maps differ $\eta$ attributes, $\eta \leq \lambda$. Let $\text{AttrSet}$ be the quasi-identifier of $\eta+k$ K-anonymous protection models, where $\text{AttrSet}^{\eta+k}, i = 1, \ldots, (\eta+k), k \leq |q| - \eta$, and $q$ is sensitive threshold equalization control attribute sets of QI. If $P(\text{AttrSet}^{\eta+k}, q)$ is a uniform window partitioned into $\eta+k$ time axes, the transfer probability of attribute set $q'$ is expressed as follows:

$$P(q \rightarrow q') = \sum_{i=1}^{\eta+k} \left[ \sum_{j=1}^{(\eta+k)} P(\text{AttrSet}_{i-j}, q') \right] \quad (3)$$

Where, $\text{Pr}_{i}^{\lambda, \eta}$ indicates that attribute anonymous encryption in cloud computing enables hierarchical equalization of transport channel offset vectors, as follows:

$$\left[ \left( \frac{(\eta+k)}{\eta} \right) \right] \sum_{i=1}^{\eta+k} \left[ \sum_{j=1}^{(\eta+k)} P(\text{AttrSet}_{i-j}, q') \right] \quad (4)$$

When $\lambda$ increases by 1, the adaptive equalization parameters of anonymous data with $n$ input control hyperbolic cyclic mapping are satisfied:

$$\text{Pr}_{i}^{\lambda+1, \eta} = \frac{\left( \frac{(\eta+k)}{\eta} \right)}{\text{Pr}_{i}^{\lambda, \eta}} \cdot \frac{(\lambda+1)(m-\lambda+1)}{(\lambda+1-\eta-k)(m-\lambda+1-|q|+\eta+k)} \quad (5)$$

Where, $1 \leq \frac{\text{Pr}_{i}^{\lambda+1, \eta}}{\text{Pr}_{i}^{\lambda, \eta}} \leq \lambda+1$, and $\eta+k \leq \min(\lambda, |q|)$. The low bandwidth and wide stationary characteristics of the K-anonymous protection model is used, there exists $P(q \rightarrow q')$, with the increase of $\lambda$, $P(q \rightarrow q')$. According to the above hyperbolic cyclic mapping anonymous cloud computing data anonymous encryption mechanism system, combined with the balanced scheduling principle, cloud computing data anonymous encryption optimization design is carried out[10].

### 2.2. Priority List Control

The priority list control model for anonymous cloud computing data encryption based on hyperbolic loop mapping is composed of a cluster head, several cooperative cluster heads and cluster members. The structure model of priority list control is shown in figure 2.
Figure 2. Structure model of priority list control for attribute encryption

Setting the test set managed by the anonymous big data process for hyperbolic loop mapping as \( p_i \), the priority attribute \( DR(p_i,n_j) \) for performing data encryption and anonymous protection tasks \( n_j \) in cloud computing is defined as:

\[
DR(p_i,n_j) = rwd_{\lambda} \times PET(p_i,n_j)
\]

(6)

The a-diversity input control parameter of anonymous cloud computing data encryption based on hyperbolic loop mapping is described. The delay equalization is done by using the difference of transmission time between scheduling tasks, so as to realize the closeness of cluster nodes. In order to reduce the delay of data encryption in cloud computing environment, \( o_{\mu} = 0 \) is used to analyze time series in scheduling time window and privacy protection protocol[11], and the average mutual information mapping of time series \( \{x_n\}_{n=1}^{\mu} \) in feature space:

\[
x_n = [x(0), x(1), L, x(N-1)]
\]

(7)

The difference between the cloud computing data anonymous encryption clustering nodes and sink nodes is calculated, and the closeness of clustering nodes is measured[12]. The relative correlation characteristic function of attribute anonymous encryption in cloud computing environment is described as:

\[
AT(v) = \max_{u \in F(u)} [AT(u) + delay(v)]
\]

(8)

In the formula, \( A \) represents a scale amplitude value, \( delay(v) \) represents the delay of data encryption under the cloud computing environment, and in the time period \( T \), the double-curve cyclic mapping anonymous large data attribute is a random variable set with self-correlation, and priority list control model is described as:

\[
B(q') = \sum \left[ \frac{\sup_{p_{\mu}(q)} \left( p(q \rightarrow q') - p(q' \rightarrow q) \right)}{\sup_{p_{\mu}(q')}} \right]
\]

(9)

\[
Var(B(q')) = \sum \left[ \frac{\sup_{p_{\mu}(q)}}{\sup_{p_{\mu}(q')}} \left( p(q \rightarrow q') - p(q \rightarrow q')^2 \right) \right]
\]

(10)

According to the above priority list, changing the value of \( \lambda \) to control the equalization of attribute anonymous encryption.

3. Improved Design and Implementation of Anonymous Encryption Algorithm

3.1. Channel Model of Load Balancing Transmission

On the basis of constructing the priority list control model of data encryption in cloud computing environment, the improved data encryption algorithm in cloud computing environment is designed, and an anonymous cloud meter with hyperbolic cyclic mapping is proposed. The algorithm uses bilinear differential control protocol to implement load balancing control and encryption key design of anonymous big data for hyperbolic cyclic mapping[13]. By slot allocation, the load of the \( i \)-time transmission cluster scheduling unit meets the following requirements:

\[
\sum_{n=1}^{M} x_{ni} \geq N \quad i \in [1, N]
\]

(11)
In this case, the energy allocation control function in the attribute anonymous encryption model in cloud computing environment satisfies:

$$\overline{D} = \frac{\sum_{i=1}^{n}|P_i|}{\sum_{i=1}^{n}|L_i|}$$

(12)

Where, $P_i$ is the compactness measure of slot allocation control. Through leading slot allocation, data transmission relay nodes are divided into $K$ subsets of data, and bilinear differential in attribute anonymous encryption in cloud computing environment is obtained[14]. The control protocol is expressed as:

$$\begin{cases} x = (x_1, x_2, \ldots, x_n) \\ y = F(x) = (f_1(x), f_2(x), \ldots, f_m(x))^T \end{cases}$$

(13)

Where, $x = (x_1, x_2, \ldots, x_n)$ is a set of distributed cooperative cluster units, $y = F(x)$ represents the $p$-sensitive attribute function. Assuming that the class of attribute set $n_i$ of the initial micro data table is $r_j$, then the identifier attribute sampling set $P(n_i) = \{p_{ij} \mid p_{ij} = 1, k = 1,2, \ldots, m\}$, by the minimum density redundant node coverage and information recombination, the load balancing transmission description in the data scheduling process is obtained as follows:

$$M_v = w_1 \sum_{i=1}^{\max}(H_i - S_j) + M_w \sum_{i=1}^{\max}(S_j - V_i)$$

$$+ w_s \sum_{i=1}^{\max}(V_i - H_i)$$

(14)

The fitness function of control for bilinear differential control protocol is:

$$f_o = w_i \delta_i + w_c \delta_c + w_p \delta_p + w_q \delta_q$$

(15)

Where $w_i + w_c + w_p + w_q = 1$, the channel model of load balancing transmission is constructed, and the design of adaptive attribute encryption anonymous control is carried out.

### 3.2. Optimal Implementation of Adaptive Attribute Encryption Anonymous Algorithm

Based on load balancing control and encryption key design of hyperbolic cyclic map anonymous big data using bilinear differential control protocol, the key function of anonymous encryption for cloud computing data is constructed by combining adaptive weighting control method:

$$x = \sum_{i=1}^{N} s_i \Psi_i = \Psi_s, \Psi = [\Psi_1, \Psi_2, \ldots, \Psi_N]$$

(16)

The time window weighting control of attribute encryption anonymous control for big data assignment task node $i$, the weighting function is:

$$\begin{cases} x_{id}^{(t+1)} = v_{id}^{t} + c_1 \cdot r_1 (p_{id}^{t} - x_{id}^{t}) + c_2 \cdot r_2 (p_{end}^{t} - x_{id}^{t}) \\ x_{id}^{(t+1)} = x_{id}^{t} + v_{id}^{(t+1)} \end{cases}$$

(17)

The adaptive weight coefficient is adjusted in the node link. The updating mechanism of the weighting coefficient is obtained as follows:

$$v_{id}^{(t+1)} = w \cdot v_{id}^{t} + c_1 \cdot r_1 (p_{id}^{t} - x_{id}^{t}) + c_2 \cdot r_2 (p_{end}^{t} - x_{id}^{t})$$

(18)

The time window and the privacy protection protocol are optimized by time slot allocation, and the optimal control model for anonymous encryption of cloud computing data is obtained as follows:
\[
\begin{align*}
  d_{\text{mean}}(t) &= \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} d_{ij}(t)}{n \times d} \\
  d_{\text{max}}(t) &= \max \left\{ d_{ij}(t) \right\} \\
  k &= \left| d_{\text{max}}(t) - d_{\text{mean}}(t) \right| / d_{\text{max}}(t)
\end{align*}
\]

Where, the execution overhead of anonymous encryption of cloud computing data is:

\[
\begin{align*}
  w = w(t) * w_{\text{start}} & \quad k \geq \alpha \\
  w = w(t) * \frac{1}{w_{\text{end}}} & \quad k < \beta
\end{align*}
\]

The channel utilization is expressed as:

\[
u_i = \frac{1}{N} \sum_{i=1}^{N} u_i = \frac{1}{MN} \sum_{m=1}^{M} \sum_{i=1}^{N} x_{mi}
\]

In the above formula, \(\{\alpha, \beta\}\) is the directivity function of task execution for the m time slot, the time window and privacy protection protocol of attribute encryption and anonymity control is optimized with slot allocation, thus Cryptographic anonymous algorithm is improved [15-17].

4. Test and Analysis of Simulation Experiment

In order to test the performance of this algorithm in the implementation of anonymous cloud computing data encryption with hyperbolic cyclic mapping, simulation experiments are carried out. The simulation experiment is established in the environment of Matlab 7. The simulation experiment uses NS-2.27 and NS software to simulate the anonymous big data information flow of hyperbolic cyclic mapping. The random function generator is used to generate big data information and the big data information is sampled. The sample length is 1024, and 10 data sets are used to do the experiment. The relative error of attribute anonymous encryption in cloud computing environment is calculated to be \(\left| \text{Ans}(\text{query}, D) - \text{Ans}(\text{query}, D') \right| / \text{Ans}(\text{query}, D)\) and the data recall rate is taken as the test index. According to the above simulation environment, the data is adjusted. Simulation analysis shows that the sampled big data information flow is shown in figure 3.

![Figure 3. Anonymous big data time-domain waveform of hyperbolic cyclic mapping](image-url)
The sampled data set is taken as the test sample and combining the adaptive weighting control method to control the anonymous encryption of cloud computing data, the time window and privacy protection protocol of attribute encryption and anonymous control are implemented through time slot allocation. In order to compare the performance, different algorithms are adopted, and the relative error and recall rate of data scheduling are taken as the test performance index. The comparison results of scheduling performance with different algorithms are shown in figures 4 and figure 5.

![Figure 4. Relative error of data encryption](image)

**Figure 4. Relative error of data encryption**

![Figure 5. Comparison of data encryption recall rate](image)

**Figure 5. Comparison of data encryption recall rate**

By analyzing the simulation results above, it is shown that the proposed algorithm is used for attribute anonymous encryption in cloud computing environment, and the relative error of data scheduling is effectively reduced by adaptive attribute encryption anonymous control. The error converges to zero and the number of data is reduced to zero. The recall rate is much higher than the traditional algorithm, which proves the superior performance of this method.

5. Conclusions
In order to improve the self-adaptability and accurate control of data encryption in cloud computing environment, an anonymous data encryption algorithm based on hyperbolic cyclic mapping is proposed. The priority list control model of adaptive privacy protection for cloud data is constructed. The load balancing control and encryption key design of anonymous big data with hyperbolic cyclic mapping are implemented by using bilinear differential control protocol. The hyperbolic differential equation control and adaptive weighting method are used to construct the key function for anonymous encryption of cloud computing data. The time window and privacy protection protocol of attribute encryption anonymous control is optimized by slot allocation. The encryption anonymous algorithm is improved. Simulation results show that the adaptive equalization performance of attribute anonymous encryption in cloud computing environment is better, the ability of anti-attack is better, and the recall rate of data is better than the traditional method. This method has good application value in cloud data anonymous encryption and privacy protection.

6. References
[1] ZHANG Q Y, WANG R C, SHA C, et al., (2013). Node correlation clustering algorithm for wireless multimedia sensor networks based on overlapped FoVs. Journal of China Universities of Posts and Telecommunications, 20(5), pp. 37-44.
[2] LIU Z, YUAN Y, GUAN X, et al., (2015). An approach of distributed joint optimization for cluster-based wireless sensor networks. IEEE/CAA Journal of Automatica Sinica, 2(3), pp. 267-273.
[3] YANG Jing-ming HOU Yu-hao SUN Hao, et al., (2016). Modified NSGA-II-DE with
two-dimensional information ordering strategy and magnitude threshold. Control and Decision, 31(9), pp. 1577-1584.

[4] GUSTAVO MARFIA, MARCO ROCETTI, ALESSANDRO AMOROSO, et al., (2013). Safe Driving in LA: Report from the Greatest Intervehicular Accident Detection Test Ever. IEEE Transactions on Vehicular Technology, 62(2), pp.522-535.

[5] YAN Z, LIU L, (2010). Method of program automatic parallelization based on data dependence. Journal of Jilin University (Science Edition), 48(1), pp. 94-98.

[6] CAO Yu-lin, WANG Xiao-ming, HE Zao-bo, (2016). Optimal Security Strategy for Malware Propagation in Mobile Wireless Sensor Networks. Acta Electronica Sinica, 44(8), pp. 1851-1857.

[7] Chang YL, Lin TL, (2012). Network-based H.264/AVC whole frame loss visibility model and frame dropping methods. IEEE Transactions on Image Processing, 21(8), pp.3353-3363.

[8] CAO Yu-lin, WANG Xiao-ming, HE Zao-bo, (2016). Optimal Security Strategy for Malware Propagation in Mobile Wireless Sensor Networks. Acta Electronica Sinica, 44(8), pp. 1851-1857.

[9] Qinsheng Du, Baohua Jiang, (2012). Design and Implementation of the Embedded Based Web Camera System. Journal of Software, 7(11), 2560-2566.

[10] H HARTENSTEIN, K P LABERTEAUX, (2008). A Tutorial Survey on Vehicular Ad Hoc Networks. IEEE Communications Magazine, 46 (6), pp.164-171.

[11] P. Samarati., (2001). Protecting respondents’ identities in microdata release. IEEE Transactions on Knowledge and Data Engineering, 13(6), pp.1010-1027.

[12] Alfaro V M, Vilanova B R, (2013). Robust tuning of 2DoF five-parameter PID controllers for inverse response controlled processes. Journal of Process Control, 23(4), pp. 453-462.

[13] Chenwei Deng, Weisi Lin, (2011). Performance analysis, parameter selection and extensions to H.264/AVC FRExt for high resolution video coding. Journal of Visual Communication & Image Representation, 22(8), pp. 749-759.

[14] XIA K, WU Y, REN X, et al., (2013). Research in Clustering Algorithm for Diseases Analysis. Journal of Networks, 8(7), pp. 1632-1639.

[15] Xia K, Cai J, Wu Y, (2012). Research on Improved Network Data Fault-Tolerant Transmission Optimization Algorithm. Journal of Convergence Information Technology, 7(19), pp.208-213.

[16] CUN Yong-jun, ZHNAG Yong-hua, (2015). Linux System Dual Threshold Scheduling Algorithm Based on Characteristic Scale Equilibrium. Computer Science, 42(6), pp.181-184.

[17] SUN Sanshan, WANG Shuai, FAN Zifu, (2016). Flow scheduling cost based congestion control routing algorithm for data center network on software defined network architecture. Journal of Computer Applications, 36(7), pp. 1784-1788.