Research on the personal privacy information protection problem based on computer security technology

Shuangxi Zhong [1], Min Zhang [2]*

[1]School of Economics and Management, Jiangxi University of Traditional Chinese Medicine, Nanchang, 330004, China

[2]School of Economics and Management, Jiangxi University of Traditional Chinese Medicine, Nanchang, 330004, China

* Corresponding author, e-mail: min_zhang2014@yeah.net

Keywords: Personalized anonymity; Public key system; Particle swarm; Group signature; K-anonymity; L-diversity

Abstract. In order to improve the security of the individual privacy data, personal privacy information computer protection method has been designed using the public key system and the group signature, which adopted personalized privacy anonymity technology, and combined with the particle swarm algorithm. This method has orderly arranged personal privacy information by anonymous and non anonymous, the information sequence that needed key security encryption has finally obtained according to the security level. It is found that this algorithm is better than two kinds of protection model k-anonymity and l-diversity in the aspect of the protection limitation of personal privacy information, through the security attack test in the same period of time, the protection number using this algorithm is also more than others . It is a very University security protection method for computer privacy , which can effectively resist five types of attacks that contains links, homogeneity, background knowledge, skewness and approximate.

Introduction

With the rapid development of Internet, data storage and computer technology, the collection and analysis of information is more complete, convenient and accurate, but there will be some risk of privacy information leakage in the process of data release, such as the release of some information sharing, data mining, knowledge discovery ,etc. For these reasons, it has become the study focus that privacy protection problem in the data publishing process, so we need to protect the information the original of the data contains, under the premise of ensuring the data availability, which can enhance the release of data security, and ultimately enable the balance relationships between privacy protection and the data availability. This paper has made a study of personalized anonymity technology in data publication in many ways, and mainly personalized requirements for service in the privacy protection, which ensure the information strong usability problems. The information protection has been designed using the model of particle swarm algorithm, the process is shown in figure 1.

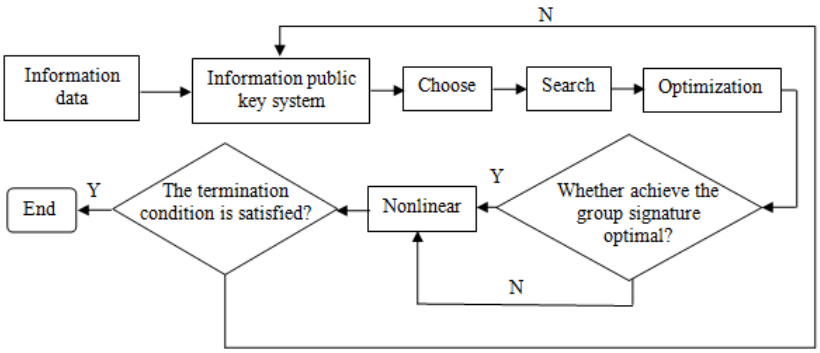

Fig.1: The computer protection overall framework of personal privacy

The computer protection overall framework of personal privacy that designed in this paper is shown in Figure 1. The protection of personal privacy information is mainly using particle swarm algorithm for code, the coding process includes selection, search and optimization. When the individual privacy data sequence that has been coded encoded is optimal, the algorithm terminates if the termination condition is satisfied. Otherwise, the particle swarm optimization algorithm will be used again for information ranking according to security levels, finally the privacy data sequences with different security levels will be got.

Design of personal privacy information personalized anonymity protection algorithm

With the popularity of the Internet, once the privacy of personal information was leaked, it would spread very strong. In order to prevent leakage of personal information, and strengthen the computer protection of personal privacy information, first of all, we need to study the information diffusion model.

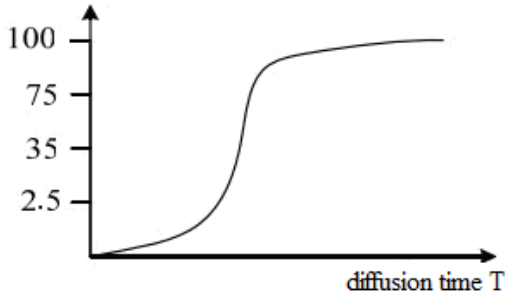

Fig.2: The information diffusion model

The diffusion model information has been shown in Figure 2, it can be seen from the chart that in the diffusion is not high in the information initial position, the information security protection performance can be improved if the information safety protection could be strengthened in this position. In order to prevent leakage of privacy information and diffusion, the encryption of multiple information access distributed IP is needed. Suppose in a D dimension target search space, there are N IP that form a community, among them, the i particles are represented as a D dimensional vector,

$$X_i = (x_{i1}, x_{i2}, \cdots, x_{iD}), \quad i = 1,2,\cdots, N \tag{1}$$

The *i* IP access information can be written as,

$$P_i = (p_{i1}, p_{i2}, \cdots, p_{iD}), \qquad i = 1,2,\cdots 3 \tag{2}$$

In order to prevent privacy information diffusion, the encryption of information according to the privacy level is needed. Then in order to make the optimal storage space, the searching on privacy information according to sequence is needed.

$$P_{\text{best}} = (p_{i1}, p_{i2}, \cdots, p_{iD}), \qquad i = 1,2,\cdots 3 \tag{3}$$

A plurality of information sequence can be got by use of multivariate public key cryptosystem. It can be written as functions form,

$$g(P_{best}) = g(p_{g1}, p_{g2}, \cdots, p_{gD}) \tag{4}$$

Each variable of multivariate public key can be signed, group signature mathematical model of multivariate public key system can be got finally, which is shown in follow formula.

$$\begin{aligned} p_{ij}(t+1) &= cp_{ij}(t) + c_1(p_{ij}(t) - q_{ij}(t)) + c_2(p_{gi}(t) - q_{ij}(t)) \\ q_{ij}(t+1) &= q_{ij}(t) + p_{ij}(t+1) \end{aligned} \tag{5}$$

In data security defense system of cloud computing, three-tier defense system can be built combined with typical cloud computing data application model [11]. Each layer builds them own defensive wall respectively and integrates and forms an integral defense.The first layer of data security model of cloud computing mainly verifies the identity of cloud computing and configure user's rights. The second layer mainly encrypts data resources and protects user's privacy. It also

encrypts the document using chunking such as M is data resources cloud computing needed. The data M has been divided into same subset of the data matrix $M=(M_{1,}M_2,...,M_n)$ in the second layer of the security model. We can build chunked encoding matrix Y_0 of cloud computing data resources M using Vander monde matrix:

$$Y_0=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_m^{n-1} \end{bmatrix} \tag{6}$$

In formula (1), m=n+k, $\alpha_i(i\in\{1,2,...,n\})$. There are random natural numbers. Through the change of Y_0, we can get:

$$Y=(I/\beta)=\begin{bmatrix} 1 & 0 & ... & 0 & \beta_{11} & \beta_{12} & ... & \beta_{1k} \\ 0 & 1 & ... & 0 & \beta_{21} & \beta_{21} & ... & \beta_{2k} \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & \beta_{m1} & \beta_{m1} & & \beta_{mk} \end{bmatrix} \tag{7}$$

In formula (7), β is user password matrix of cloud computing. We can multiply data resources M and chunked encoding matrix A of the data resources. Cloud users can encode data resources F:

$$F=M\cdot A=(F^{(1)},F^{(2)},...,F^{(n)})=(M_1,M_2,...,M_n,F^{(1)},F^{(2)},...,F^{(n)}) \tag{8}$$

As is shown in formula (3), after the users access the encoded data resources F, it is need to recover the data resources. The third layer will play their functions to recover the data quickly. The user needs any block of data resources $F'=(F_1',F_2',...,F_m')$. F_i' is the resources stored data vector $G^{(k)}$ of stored data resource vector G. $k\in l$.l is index set of data resources of the whole F'. The matrices F' are corresponding to transformation matrix β'.Therefore, $Y=G'\cdot\beta'^{-1}$ and the recovery of data resource can be achieved.

In the formula, *c* is label, *p* is signature label function, *t* is time. The users restrictive condition is saved in XML format to the system directory, so as to read in the conditions examination behind, its programming is shown as follows.

〈Policies TargetUid="10012">
〈Policy Effect="Permit">
<Pernnission>android.permission.SEND_SMS</Permission>
〈Constraint CombiningAlgorithm="edu:android:apex:ALL">
〈Expression FunctionID="edu:android:apex:less-than-equar'>
<ApplicationAttribute AttributeName="sentMms" default="0">
<Constant>5</Constant>
〈Expression〉
〈/Constraint〉
<Update>
〈Update TargetAttribute="sentMms">
〈Expression FunctionlD="edu:android:apex;add">
<ApplicationAttribute AttributeName="sentMms" default="0">
<Constant>l</Constant>
</Expression>
</Policy>
</Policies>
.....

Research on personalized anonymity protection of personal privacy information

In order to verify the validity and reliability of personal privacy personalized anonymity algorithm that designed in the previous chapters, the form of computer attack has been adopted to attack on anonymity personal information, the public key system of personal privacy information is firstly established, which is shown in figure 3.

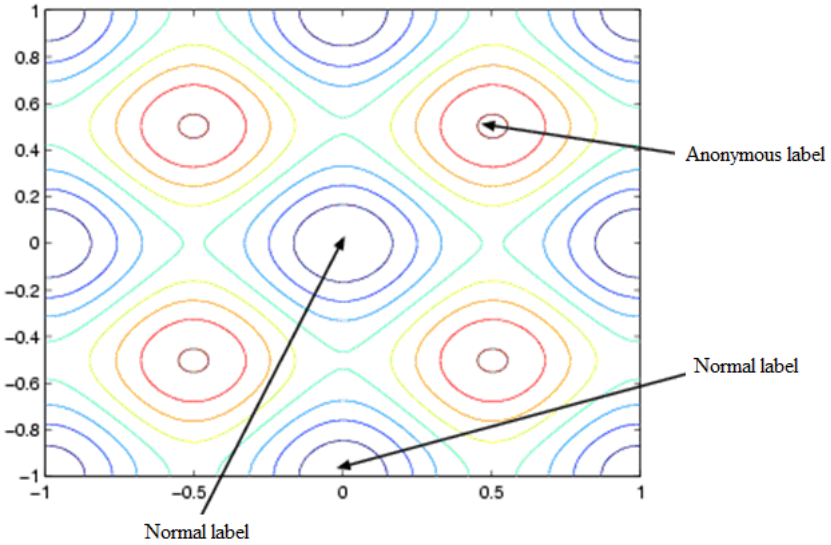

Fig.3: Schematic diagram of variable public key cryptosystem

The schematic diagram of personalized anonymity privacy protection is shown in Figure 3, in the limited storage space, the personal privacy information has been orderly arranged according to the anonymous and non anonymous, personal information that needed protection and public information has been arranged, finally we can get information sequence that needed priority security encryption.

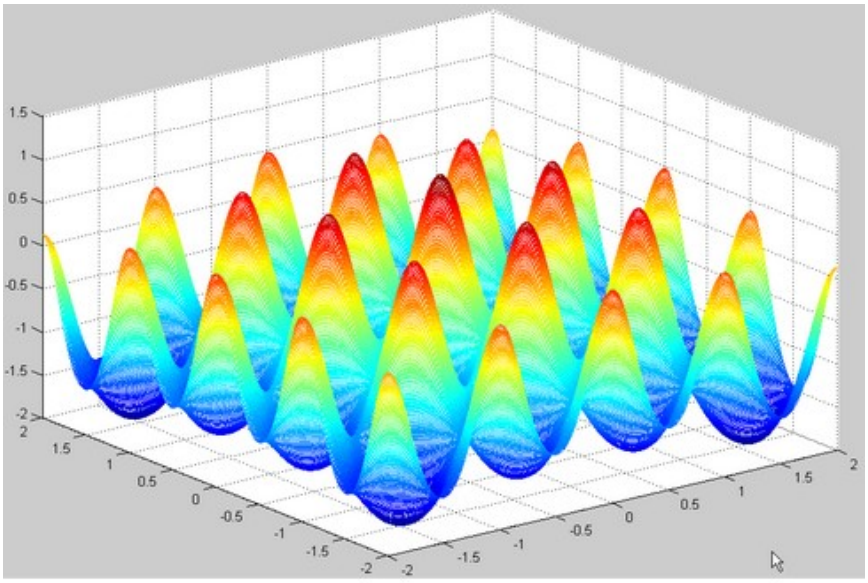

Fig.4: The results of group signature security level

Figure 4 shows final safety level sketch map, after the encoding for the individual privacy information using variable public key cryptosystem, then statistical computing of the security level using group signature technology. When the information code is negative, privacy security can not be considered, but when the privacy safety information value is more than 1, double encryption is needed.

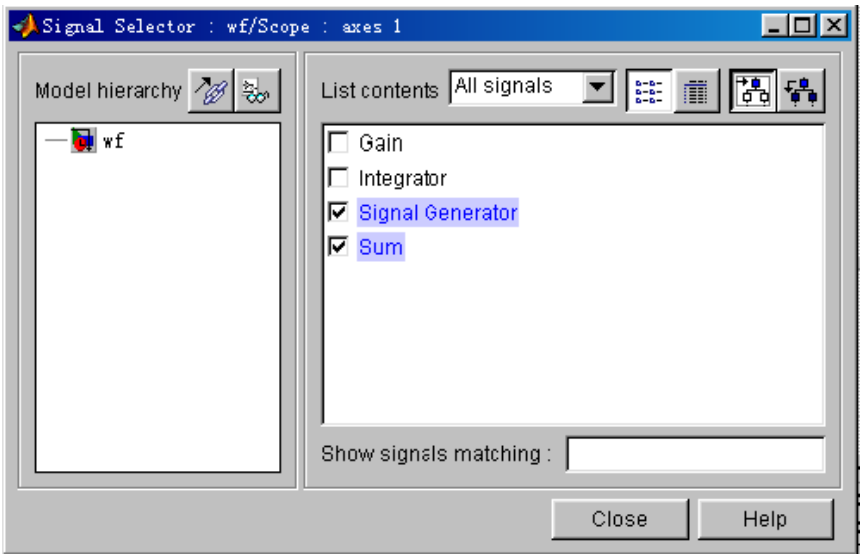

Fig.5: The curve window of generation security detection

The curve window of generation the detection signal according to the computation time is shown in Figure 5. In order to verify the effectiveness and efficiency of the privacy information protection method that designed in this paper, Matlab software is used for computing of safety protection time of an attack, the aging curves of different models has been obtained through simulation and curve fitting, as shown in Figure 6.

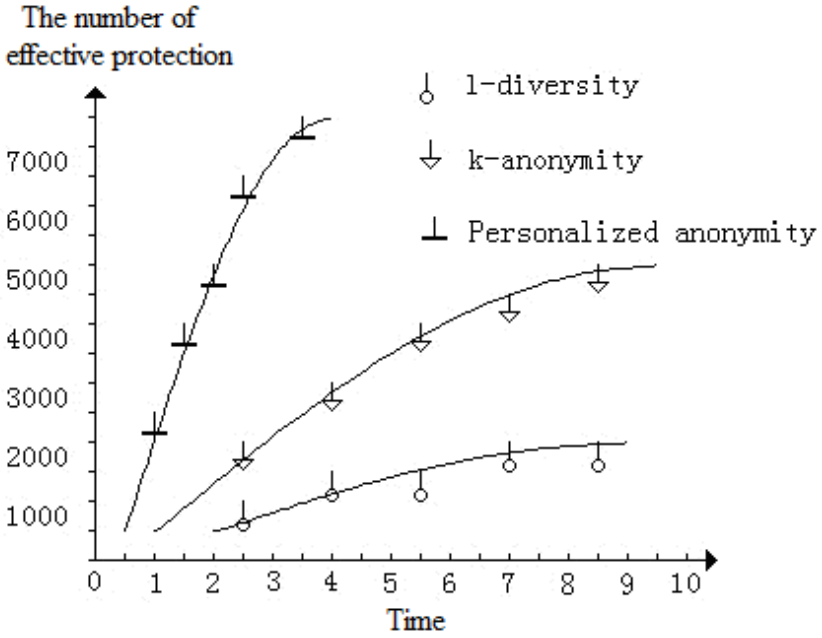

Fig.6: The protect aging curve under different algorithms

Figure 6 shows the aging curve protection of personal privacy information under different algorithms, it can be seen from the chart, the aging protection that using personalized anonymity method is better for personal privacy information, compared to two kinds of protection model k-anonymity and l-diversity, the number of effective protection is higher at the same time.

Tab 1: The experimental results of different privacy protection technology

Protection model	Link attack	Homogeneity attack	Background knowledge attack	Skewness attack	Approxi-mation attack
k-anonymity	√		√		
l-diversity	√			√	
t-closeness	√	√			
m-invariance	√				√
personalized anonymity privacy protection model	√	√	√	√	√

Table 1 shows the final effective experimental data using five kinds of attack types for the attack individual privacy data, it is shown form the experimental results that the personalized privacy anonymity protection model is superior to other computer protection model, which can effectively resist five attack types of link, homogeneous, background knowledge, skewness and approximation. It is a very effective computer security protection method, which can be extended to the privacy data protection scheme for more types.

Conclusion

First, the personalized anonymity technology has been used in this paper, the particle swarm mathematical model of computer security privacy protection has been designed using the public key system and group signature, the particle mass function of different security levels has been obtained, and the XML algorithm has been programmed in this paper.

Secondly, in order to verify the validity and reliability of the algorithm, personal privacy information security attacks is adopted to attacks on personalized anonymity privacy data, the data protection time curve and validity result under different algorithm has been obtained in this paper.

In the end, through the analysis of the aggressive behavior data and the protection results, it is found that the algorithm presented in this paper has the number of protection is higher than others at the same time, and can effectively resist five attack types of the link, homogeneous, background knowledge, skewness and approximate, which is a reliable computer security protection algorithm.

References

[1] Li Yuxiao. The privacy protection brook no delay in the age of cloud computing big data. Theory review. No.07, (2013), p.10

[2] Zhou Hailing. Protection of network infringement and privacy. Journal of Henan Normal University (Philosophy and Social Sciences Edition). Vol.40, No.1, (2013), p.43-45

[3] Luo Jinli at the age of big data, awkward user privacy. Financial Times of science and technology. No.12, (2012), p.26

[4] Yi Bin, Pan Yanan. Discussion on the network of personal information privacy authentication mechanism. Information theory and practice,Vol.35, No. 05, (2012), p.41-43,68

[5] Li Zheng Shi, Quanyou. South Korea electronic commerce development research. Strategic decision-making research. Vol.2, No.5, (2011), p.19-24

[6] Xiao Zibi, Yang Bo. The protection of personal privacy in electronic commerce issues and technology research. Journal of Wuhan Metallurgical Manager's Institute. Vol.20, No.3 (2010), p.10-12

[8] Jiang Ling. Analysis of America children's online privacy protection. Sichuan Library Journal. No.05, (2009), p.77-80

[9] Zhou Tao. A study of website privacy statements based on content analysis method. Journal of Hangzhou Dianzi University (Social Science Edition). Vol.5, No.3, (2009), p.11-16

[10] Wang Liming. Protection of personality right under the network environment. Journal of China University of Geosciences (Social Science Edition). Vol.12, No.4 (2012), p.1-7

[11] Li Chengyuan, Fan Hong, Li Haitao, Han Yu. The technical research of entire protection of Cloud platform information security. Information security and technology. No.9, (2011), p.65-70
[12] Chen Kang, Zheng Weimin. Cloud Computing: System instances and current research. Journal of Software. Vol.20, No.5, (2009), p.1337-1348
[13] Wu Xudong. Cloud computing data security research. The twenty-sixth national computer security academic exchanges. No.9, (2011), p.38-40