Data Security Scheme for a Trusted Third Party Platform Based on RSA One-time Key

To cite this article: Zhiqiang He *et al* 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **234** 012046

Data Security Scheme for a Trusted Third Party Platform Based on RSA One-time Key

Zhiqiang He[1,2,], Nengneng Li[1,2,*] and Xiwei Xu[1,2]

1. Weifang Vocational College
2. No.06588, Hai'an Road, Science and Education Innovation Park, Binhai Economic and Technological Development , Zone, Weifang City, Shandong Province, 262737, China.
*E-mail: linengneng1992@163.com

Abstract—In recent years, the possibility that cloud data is accessed illegally and the key is cracked in the process of storage is becoming increasingly. The paper proposes a data security scheme of a trusted third party platform based on RSA one-time pad encryption technology. It can use RSA one-time pad encryption technology to realize the function that encrypt the data in security. Then it manages the one-time key generation by the trusted third party platform. Finally, the simulation experiment detected the data security by using the MD5 algorithm and compared the digital fingerprint generated by the data before being attacked and after being attacked. The experimental results show that this scheme increases the workload of the key cracking, and reducing the probability of key being cracked and data being accessed illegally.

1. Introduction

In recent years, with the emergence of cloud service providers in large quantities, more and more enterprises, organizations and individuals store data to the cloud to manage, which depends on the cloud computing data storage and high-speed computing features. However, the extensive application of cloud computing has brought security risks for the user's data. At the same time, as the service providers management system and the level of service provided is different, the user can not determine which cloud service providers are reliable [1].

At the end of 2012, the famous enterprise VMware announced the third annual cloud heat survey. 70% of users refused to use the cloud. The main reason is worried about cloud information security and privacy issues. This shows that security and privacy issues have become the biggest obstacle to the development of cloud services [2]. In addition, after the data storage into the cloud, the data of the various operations are carried out in the cloud. Cloud service providers have too much authority so that increasing the user's distrust of this. For the above two issues, this paper presents a third-party platform based on a RSA Once a trusted. It not only to the problem of unauthorized theft of the key and ensure the security of encrypted data, but also share part of the work of the cloud and weaken the cloud service providers permission. In addition, trusted third-party platform in addition to having the function of the key management and storage of user information, can record data access information, and in contrast to the cloud record for finding any one of the illegal data access quickly.

2. Cloud Data Security Analysis

2.1 Cloud computing data and privacy security

One of the characteristics of cloud computing is to provide services to users through the Internet. The users storage all the data into the cloud, and send the results to the client through the network. Cloud computing as a new service model, facing the risk is unprecedented in aspect of data management. In order to improve the efficiency of the use of resources, users need to co-calculation and use of shared resources. If the user is not a good isolation between the measures, then the data will face the threat of stealing, deleting, and tampering. The security risks faced by the data are summarized as follows:

1. Date storage security

Data storage is an important part of the data security lifecycle. The enterprise saves the data in the cloud. This includes the storage location of the data, the isolation of the data and the disaster recovery of the data. These are the security aspects to be considered in the data storage. However, the user does not know which server is trusted and the data is stored on that server, and can the cloud service provider guarantee that the enterprise data is not leaked.

2. Data transmission security

Under normal circumstances, the data of enterprises transmission to the cloud service providers to deal with is extremely confidential. They are on behalf of the enterprise's competitiveness, including corporate user information, corporate financial information, enterprise products and service features. However, the enterprise data transmission to the cloud service providers face several security issues. First, how to ensure that these data are encrypted strictly in the transmission process, and the data can not be restored after being stolen; Second, how to ensure that cloud service providers will not be leaked out of the data after getting it; Third, in the cloud computing service providers, how to ensure that users access are through strictly authority verified, then accessing data legally, and to ensure that enterprises can be safely accessed to their own data at any time [3].

3. Data sharing security

The user's data is stored in the cloud storage resource pool in a dynamically shared manner, losing control of its private data. And the data is exposed to the risk of disclosure and abuse. Cloud storage uses virtualization technology to share resources. Different users can store the data in the same physical device. If there is no effective access control mechanism, it can not achieve the logical isolation of the data.

2.2 Cloud computing data security protection measures

In the cloud computing, constructing of a variety of password system, password supervision, password operation and maintenance mechanisms encrypts data, to protect data not being illegal theft, modified and used in the transmission and storage process; and conducting the user access, security level and other aspects of control to ensure data security and credibility.

3. Trusted Third Party Platform

3.1 RSA once encrypted encryption technology

RSA one-time pad encryption technology is based on RSA algorithm to add a pair of keys, including an encryption key e0 and a decryption key d0 [4]. After each encryption and decryption, e0 and d0 change by its own iterative function. It does not need to generate large prime number to generate other keys, only through the new key (e0, d0) changing to achieve one time pad.

3.1.1 Logistic mapping

Logistic map [5] is also called Logistic iteration. It is a time discrete power system, that repeated iteration according to the following equation [6] :

$$x(t+1) = \mu x(t)(1-x(t)) \tag{1}$$

Among them t is an iteration time step, and for any t, x (t) ∈ [0,1]. μ is an adjustable parameter. In order to ensure that the mapping x (t) is always in [0,1], μ> 3. When the parameter μ changes to a different value, the stability point, period and chaos of the equation are different.

Here we only introduce the case when μ> 3.

When 3 <μ <3.6, the iteration of the equation will occur in periodic behavior. As the μ increases, the length of the cycle increases accordingly. As shown in Figure 1, the left cycle is 2 and the right side is 4.

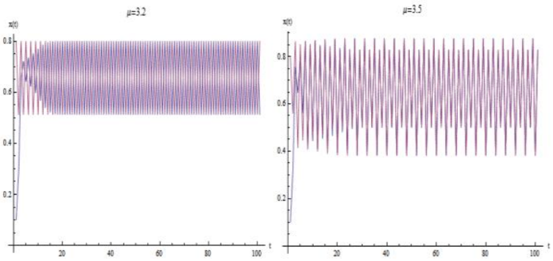

Figure. 1 μ =3.2 AND μ =3.5

We can see from the figure, when μ is 3.2, the graphic appear jagged. The value of x(t) is hovering up and down at 0.5 and 0.8. Although starting from a different initial value (blue and purple lines), the evolution of the system is not same, their final values are always 0.5 and 0.8.

Figure 2 shows that μ = 3.5, the system is repeatedly flapping between the value ofin the 0.87 -> 0.4 -> 0.82 -> 0.5. The two tracks (blue and purple) are slightly different at first, but eventually converge together. If further increasing the value of μ, the system will show more than 8 cycles, 16 cycles and more.

Figure 3 shows the change when μ = 3.6. Starting from μ = 3.54, as the μ increases, the system shock cycle will become longer and longer. Until μ is about 3.6, the length of the cycle will tend to infinity. At the same time, the system began a chaotic state. We can compute the statistical distribution of the x (t) values at different times in the interval [0.3, 0.9]. The results are shown in Figure 3 below:

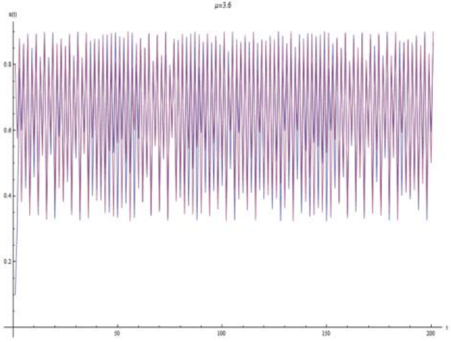

Figure. 2 μ =3.6

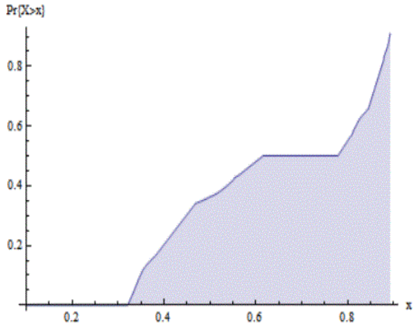

Figure. 3 The Distribution of X (T) Over The [0,1] Interval

The graph shows the cumulative distribution of the value of x (t) at this different time on the [0,1] interval at the situation of a simulation test running 20,000 cycle. The platform part of the graph represents that the probability is essentially zero. That is the value of x (t) is concentrated in the range of [0.3, 0.6] and [0.8, 0.9]. And to the right in accordance with the line part of the tilt that x (t) is similar to the distribution of uniform in this interval. Thus, this time the iteration system shows randomness, the whole iterative equation is deterministic. So we say that there is a certainly of chaos.

3.1.2 Encryption process

The one-time encryption technology is based on the RSA encryption technology to add a pair of new keys (e0, d0), that is encryption key e0 and decryption key d0. After each encryption and decryption, (e0, d0) will be changed by its own iterative function, so there is no need to re-generate large prime to generate other keys , only through the new key (e0, d0) changes to achieve a secret. However, in order to make the added key still be able to correctly encrypt and decrypt, we must ensure that the sum of e0 and d0 is a multiple of n after each encryption, and initialization can take e0=n-d0. The following describe RSA encryption algorithm based on one-time encryption and decryption process [7].

The first is the key generation:

(1) Select the prime p and q, calculate n = pq, p and q are confidential, n is open.

(2) Calculate Φ (n) = (p-1) (q-1), let 2 ≤ e ≤ Φ (n), and gcd (e, Φ (n)) = 1, e is the encryption key.

(3)Calculate d, let ed = 1 (mod (Φ (n)), and let d be the inverse of e for modulo Φ(n), where d is the decryption key and is secret.

(4)Initialize e0, d0. As follows: In the above section we briefly introduced the basic idea of Logistic mapping and the system changes with the change of μ. In this case, initialize e0(2 ≤ e0 <n) using chaotic sequences generated by Logistic mapping.

The discrete model of Logistic map is:

$$x_{t+1} = \mu x_t(1 - x_t) \qquad 1<\mu<4, 0<x0<1, t=1,2\ldots, \tag{2}$$

It is shown that the μ in the formula (1) tends from 3 to 4, and the sequence period generated by the Logistic map leads to chaos. As long as the appropriate μ value is given, the sequence satisfying the chaotic characteristic can be generated.

(5)To {e, e0, n} for the public key, {d, d0} for the secret key.

Followed by the encryption process:

When encrypting, the plaintext bit string is first grouped so that the decimal number corresponding to each packet is less than n, that is, the packet length is less than log2n. And then we conduct encryption operation for each plaintext group m:

$$c = (m^e + e0) \bmod n \tag{3}$$

Finally, the decryption process:

$$m = (c + d0)^d \bmod n \tag{4}$$

The key change process is to generate a random integer v. After all plaintext packets are encrypted, use the following iteration function to change e0:

$$e0_{t+1} = e0_t \cdot (e + v) \bmod n \qquad n, t=0,1,2,\ldots, \tag{5}$$

After all ciphertext packets have been decrypted, use the following iteration function to change d0:

$$d0_{t+1} = d0_t \cdot (e + v) \bmod n \qquad n, t=0,1,\ldots \tag{6}$$

3.2 Design of trusted third party platform based on RSA

The traditional one-time encryption strategy based on the RSA algorithm is performed between the client and the cloud [8]. The specific flow chart shown in Figure 4.

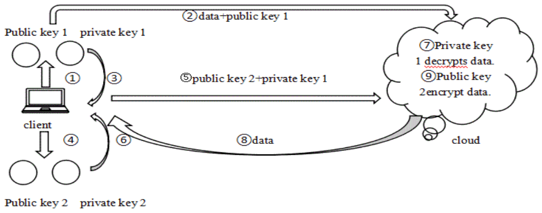

Figure. 4 Based On Rsa Algorithm for a One-Time Encryption Strategy Flow Chart

The specific process can be described as:

1) When the user first stores the data, the client's individual key management module generates a pair of public key 1 and private key 1;

2) Send the data and the public key 1 to the cloud, encrypt and store;

3) Store the private key 1 in the client;

4) Generate a pair of new RSA key, public key n and private key n when needing to read the data each time;

5) Send the new public key and the old private key to the cloud;

6) Store the new private key in the key management module;

7) Decrypt the data with the old private key in the cloud;

8) Send the decrypted data to the client;

9) Finally, re-encrypt the data with the new public key.

In this way, even if the old private key is intercepted, data can not be obtained because the data has been re-encrypted by the new public key, and the new private key that can read it has not yet been sent to the cloud.

In this process, reduce the burden on the client and make up for deficiencies that other algorithms are inefficient using powerful cloud computing capabilities. However, all the encryption and decryption process conducting in the cloud, and now the cloud service special architecture, make the cloud service provider's power be too large and too concentrated. Many users are more and more no sense of trust, but have to use this service. In this case, we can propose a trusted third-party platform based on the RSA one-time key encryption technology. The trusted third-party platform can share the work of the cloud and reduce the authority of cloud providers. And it can record through accessing the data, and can find illegal operation of data timely, and can not cause the data leakage because of the cloud platform being attacked [9-11].

Trusted third-party platform based on the RSA one-time key is to combine RSA one-time encryption technology and third-party platform, not only maintain the advantages of a trusted third-party platform itself, but also add the advantage that RSA one-time encryption algorithm can make the key be cracked more difficultly, and make the data not be illegally accessed.

3.3 The System Architecture of Trusted Third Party Platform Based on RSA

This paper presents a trusted third-party platform based on RSA, which includes three parts: client, cloud and trusted third party platform. The client only sends request to upload and download data, in order to reduce the burden on the client. It does not carry out other calculations. Trusted third-party platform mainly receive client requests, store user information, manage keys and record data operations and other operations. It is a server and has its own database. The cloud stores the encrypted data and the user's information, and records the user's operation of data.

3.4 The Work Flow of Trusted Third Party Platform Based on RSA One-time key

In the trusted third-party platform based RSA system, when it manage the data security, the first application is to generate a pair of keys using RSA encryption technology and encrypt data. Every time the data is read, the key changes. Generate a pair of new keys use the above-mentioned one-time key generation process. After accessing to data, the data is re-encrypted using the mew keys. In this process, all the keys generated by RSA are stored in a trusted third-party platform and managed by the trusted third-party platform.

When uploading data, firstly, connect the client and the trusted third-party platform, and third-party trusted platform verify the user's identity. If the user uploads new data, the new data records will be added to the third-party platform database. If the user wants to modify the data, the system needs to authentic the user permissions. When the authentication and authority authentication are passed, generate a pair of keys automatically using RSA encryption technology on the trusted third-party cloud platform. The private key is stored in the database, the public key sent to the client, and then the client will send the public key and a piece of data to the cloud. The data is encrypted using the public key after being modified.

When downloading data, trusted third-party platform connects with the client, and then verify the identity of the user. If the user has the authority to read data, the user can download the data. First, obtain the data of the private key from the trusted third-party platform, and then generate a pair of new keys through RSA one-time key technology in the third-party platform. Replace the original private key with the new private key, send the new public key and the old private key to the cloud. The cloud decrypts the data with the old private key, then sent the data to the client. Finally, re-encrypt the data with the new public key.

In this process, all the data operations are recorded in the trusted third-party platform database and the cloud. the user can compare the two records at any time to find whether the data has been accessed or modified illegally. These two records can be supervised by each other to prevent any one of the data from being tampered.

4. Simulation

The experimental environment is the Inter Core 1.73 GHz CPU, 4.00GB of memory, and the operating system is the windows 10. Installed Ubuntu 16.10 on VMware Workstation10.5.2, allocated 2GB of memory. In the virtual environment, attack the data stored in the cloud to test the the probability of data being attacked successfully, which is in the situation of adding a trusted third-party platform based RSA in the storage process and in the case of unprotected technology.

In the system, firstly, use MD5 to check all the data that the client will transmitted, generate the corresponding digital fingerprint, and store the digital fingerprint in the database. Then, store the client data in the cloud server, attack on the data illegally in the storage process. After attacking, the user download the data stored in the cloud, and then check this data using MD5 again to generate the corresponding digital fingerprint. Finally, compare digital Fingerprint, calculate the probability of digital fingerprint inconsistency.

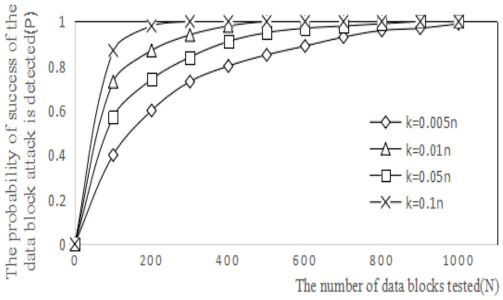

Figure. 5 The Relationship between Data Attack Success Rate and Number of Data Blocks

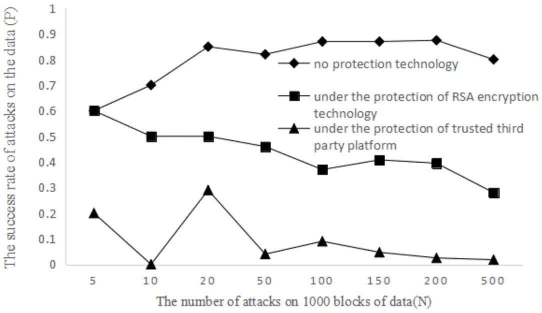

Figure. 6 Comparison of Success Rate of Data Attack Under Different Protection Techniques

Experiment 1: It is assume that each time the k-block data in the N-block data is attacked, and compare of the probability of successfully detecting a data block being attacked in the case that N is the same as k is different and N is different as k is same. The result is shown in Fig. 6. It can be seen that in the case of the total number of blocks N unchanged, the greater the number of blocks k attacked, the greater successfully detecting data being attacked; k id unchanged, the greater the N, the greater the probability that the data is successfully detected attack.

Experiment 2: According to the conclusion of experiment 1, in this experiment, attack 5,10,20,50,100,150,200 500 blocks in 1000 data. When the detection success rate is 1, detect the success rate of the data block being attacked, which is in the system of without any protection technology, the system of adding RSA encryption technology protection and the system of adding trusted third-party platform based on RSA one-time key. The results are shown in Fig7. Experiments show that the success rate of attack data in the system of adding trusted third-party platform based on RSA one-time key, and the data has higher security.

5. Conclusion

The trusted third-party platform based on the RSA one-time key presented in this paper, not only share part of the work of the cloud, reduce the cloud provider's authority and increase the user's trust in cloud computing, but also through RSA one-time key technology and the new key generated each time the data is accessed, make the illegal user not steal and crack the key, which can not read the data illegally. It forms the first layer of protection against the data. Trusted third-party platform system will store the data and keys separately; the data can not be cracked even if getting it illegally. It forms the second layer of protection against the data. Therefore, one-time trusted third-party platform based on the RSA forms two layers complete protection for data, and it can make illegal user not operate data illegally, and protect the data security.

At present, the third party platform is widely used in the business, electronics, business and payment platform. In the cloud computing data security, the market has more solutions, and third-party platform is not widely used. But by virtue of its low cost, high scalability, high availability and ensuring data security advantages, the future will have a good development prospects.

6. Acknowledgement

Weifang Science and Technology Development Plan Project, Research and Development of Data Analysis System for Higher Vocational Innovative Talents Based on Big Data (2018GX023)

7. References:

[1] Wu Han-qing.White Hat on Web Security [M]. Beijing: Electronic Industry Press, 2012.
[2] Liu Jian-Yi, WANG Zong, XUE Xiang-Dong.Safety Analysis of Cloud Storage [J]. ZTE Communications, 2012,18 (06): 30-33.
[3] Wu Xu-dong Research on Data Security of Cloud Computing [J].Information Network Security, 2011,09: 38-40.
[4] Yang Bo, He De-quan. Modern cryptography [M]. Beijing: Tsinghua University Press, 2005.4-96
[5] Fan Jiu-lun, Zhang Xue-feng. Piecewise Logistic Chaotic Map and Its Performance Analysis [J] .Journal of Electronics, 2009,04: 720-725.
[6] Lu Jin-hu. Chaotic time series analysis and its application [M]. Wuhan: Wuhan University Press, 2002.11-14.
[7] Zhang Bei, Sun Shi-liang.Second-dense encryption technology based on RSA [J] .Computer Security, 2009,03: 53-55.
[8] Wang Wei, Wu Yu-xiang, JIN Xin, LI Ning-bin.Data Security Storage Scheme Based on Trusted Third Party Public Cloud Platform [J] .Information Network Security, 2014,02: 68-74.
[9] Zhunag Ji-liang, Lin Hui-li, Li Xian-xian.Safety of Trusted Third Party Authentication Protocol [J] .Journal of Computer Research and Development, 2004,21 (12): 109-112.
[10] Wang Fei, Kang Xiao-bo.The Research on the Online Payment Mode of Bank Card Based on the Third Party Payment Platform [J]. South China Financial Computer, 2006,14 (10): 56-59.
[11] Huai Te.Hadoop authoritative guide [M]. Beijing: Tsinghua University Press, 2010