A Credible Mechanism of Service about Data Resource in Cloud Computing

Yunfa Li, Yangyang Shen and Mingyi Li
(Corresponding author: Yunfa Li)

Key Laboratory of Complex Systems Modeling and Simulation, School of Computer, Hangzhou Dianzi University
Xiasha Higher Education Zone, Hangzhou, Zhejiang Province,310018, China
(Email: yunfali@hdu.edu.cn)

(Received Feb. 25, 2017; revised and accepted May 21, 2017)

Abstract

In order to protect the security of service in cloud computing, we propose a credible mechanism of service for data resource. In the mechanism, we first build a system model and put forward its implementation process. Then, we design an encryption method used in the system model. On this basis, we discuss the function of the third party trusted platform. All of these constitute a credible mechanism of service about data resource in cloud computing. In order to verify the feasibility of the mechanism, a series of experiments have been done. The experimental results show that it is feasible to ensure the security of service about data resource in cloud computing.

Keywords: Credible; Cloud Computing; Data Resource; Service; System Model

1 Introduction

With the rapid development of virtualization technology, cloud computing begin to be widely used in data processing, data analysis. Data are usually stored to cloud server by more and more users, which leads to the scale of data resource is becoming larger and larger. In this situation, data resource are faced with more and more network attacks and the security protection of data resource is also becoming more and more difficult. In general, some traditional security maintenance methods are mainly focused on the access control strategy of data resource, the encryption and decompression method of data file, the identity authentication mechanism of data resource, data signature and so on. These technologies can play an important role in the maintenance of data security, however, as for the virtualized computing environment, these techniques and these methods exist obvious disadvantage in the maintenance of security about data resource. The main reason is that these techniques and these methods cannot make sure if the service is provided by data resource or not, which will result in the leakage or tampering of data resource information. In this state, it is very important to research the credible mechanism of data service in cloud computing [12].

Based on the above description, we will study the service mode of data resource in cloud computing in this paper. The purpose is to explore a credible mechanism of the service about data resource and maintain the security of data resource in cloud computing. Therefore, this paper is organized as follow: Section 2 overviews the literature on the security of service in cloud computing. Section 3 will proposes a credible mechanism based on the service of data resource in cloud computing. Section 4 describes a series of experiments and analyzed the results. Section 5 is the conclusion of this paper.

2 Related Works

With the rapid development of the technology of cloud computing, the scale of data resource is becoming bigger and bigger, and theirs application is becoming wider and wider. In the situation, theirs security protection is becoming more and more difficult. In order to resolve these questions, some people carried out a series of research and achieved some results. These results can be described as follows.

In [2], the authors first analyzed the challenge about the intrusion severity analysis problem for the overall security of clouds. Then, the authors presented a novel method to address this challenge and analyzed the degree of intrusion detection in clouds. On this basis, a rigorous evaluation method was presented to assess the effectiveness and feasibility of their proposed method for clouds.

The security problems faced by cloud computing and the existing security technology are described in [15]. In the paper, the authors first discussed a series of challenges faced by the security of cloud computing. Then, the authors indicated there are many methods to improve the security of cloud. At last, the authors stressed there is no one precise solutions to resolve the security of cloud

and there is facing many challenges and difficulties in the future.

In [11], the authors studied three auditing schemes for stored data including the public auditing scheme with user revocation, the proxy provable data possession and the identity-based remote data possession checking. All three mechanisms claimed that their schemes satisfied the security property of correctness. It is regretful that this comment shows that an active adversary can arbitrary alter the cloud data to generate the valid auditing response which can pass the verification. Then, they discussed the origin of the security flaw and proposed methods to remedy the weakness.

Various security challenges, vulnerabilities, attacks and threats that hamper the adoption of cloud computing are described in [17]. In the paper, the authors first provided a state-of-art survey on cloud security issues and challenges. Then, the authors explored various cloud services and what they provide as well as analyzed the security concern on each provider. At last, the authors stressed existing schemes that counter the security issues in an efficient, and cost saving manner and proposed the 3-tier security architecture for better security enhancement of cloud security.

In [7], the authors first discussed institutions and institutional evolution in the cloud industry. Then, they examined the forces and nature of institutional changes in the cloud industry. In the following section, a section on discussion and implications are described. At last, some comments are concluded.

In [8], the authors shown that Seo *et al.*'s certificateless encryption is insecure because it binds only a user's partial public key with the user's identity. An adversary can replace the remaining public key of the user to launch man-in-middle attacks. they also presented an improvement using the technique developed by Schnorr.

The security of data sharing in cloud computing is described in [6]. In the paper, an effective, scalable and flexible privacy-preserving data sharing scheme is proposed in the cloud. In order to preserve privacy and guarantee data confidentiality, a cryptographic primitive, named ciphertext policy attribute-based encryption (CP-ABE) is employed and an identity-based encryption (IBE) technique is considered.

In [9], the authors first described how to constitute an integrated security cloud platform by using the fusion technology. Then, they explained some security threats faced the cloud infrastructure. According to user's demand, the solutions to these problems are presented in detail. Finally, the technology used in the secure cloud platform is confirmed.

In [5], the authors described an efficient three-party password authenticated key exchange (3PAKE) protocols based on LHL-3PAKE proposed by Lee *et al.* The 3PAKE requires neither the server public keys nor symmetric cryptosystems such as DES. The formal proof of security of their 3PAKE is based on the computational Diffie-Hellman assumption in the random oracle model along with a parallel version of the proposed 3PAKE.

Privacy cheating discourages and secure audit protocols are proposed in [20]. Its purpose is to resolve the security and privacy problem faced by data store and computing. In the protocol, the security audit is implemented by using the technology of authentication, verification and probability sampling, which is used to verify the data stored in the data storage.

In [18], the authors presented a solution to monitor and enforce the fulfillment of secSLAs. In the solution method, a comprehensive secSLA model and a secSLA management methodology are proposed, firstly. Then, an automated remediation process for potential and actual secSLA violations is introduced. In [13], the authors first described the security challenges of data in cloud computing. Then, they presented some solutions for these challenges to overcome the risk involved in cloud computing. At last, some advanced encryption techniques and some proper key management techniques are proposed in this paper for the security of data. In [10], the authors first discussed the challenges and described the solutions for protecting big data in cloud computing. Then, they proposed an architecture named $MetaCloudDataStorage$ to protect the security of big data in cloud computing.

In order to resolve the privacy requirements of large-scale WSNs and promote energy-efficient collection of big sensor data, the authors proposed a scalable privacy-preserving big data aggregation method in [21]. In this method, sensor nodes are divided into clusters, firstly. Then, sensor data is modified by each node according to the privacy-preserving configuration message. At last, aggregated results are recovered by the sink to complete the privacy-preserving big data aggregation.

In order to research the security auditing of cloud computing, Hassan [14] first analyzed three perspectives which include user auditing requirements, the technical approaches of security auditing and the provider capabilities of current cloud service. On the basis, specific auditing issues are divided into two categories. At last, a number of techniques available to address user auditing concerns are described in the data auditing area.

In order to resolve the problem of privacy preservation, Yousra *et al.* [1] first discussed the procedures of data collection. Then, a novel anonymous technique is proposed. In the anonymous technology, a motivation model is presented and some corresponding flowcharts are analyzed. At last, the evaluation criteria of the technology are proposed.

In order to resolve the problem of data-integrity verification, Anirudha *et al.* [16] first optimize an existing third party auditing protocol. Then, a protocol to perform efficient block-level and fine-grained dynamic-data update operations is proposed on data stored in cloud computing. At last, the extensive security and performance analysis is shown.

In [4], the authors show that in the Zhu-Jiang scheme the group manager cannot complete his computational task in the registration phase. They stress that, from the

practical point of view, the mechanism that the group manager has to re-encrypt all data after a member is revoked, is not generally acceptable because it is very inefficient.

In order to study the security of data storage in cloud computing, Naresh *et al.* [19] first provided service models of cloud, deployment models and variety of security issues in data storage in cloud environment. Then, possible solutions for the data storage are described which can provide privacy and confidentiality in cloud environment.

In [3], the authors define a Storage Correctness and Fine-grained Access Provision ($SCFAP$) scheme, that provides the user an exclusive access through the use of a hierarchical structure which is a combination of users unique and common attributes. Moreover, they deploy the concept of Token Granting system that allows the users to verify the correctness of outsourced data without the retrieval of the respective files.

Although the above some methods and technologies can resolve some security questions in cloud computing, there is a lot of security problems needed to be resolved because the service mode of data resource are various and the service environment is virtual. Therefore, there are many disadvantages for the existing security technology and methods. In order to overcome these disadvantages, we present a credible mechanism of service about data resource in cloud computing.

3 The Credible Mechanism of Service

In this section, we will propose a credible mechanism in cloud computing, which is based on the service of data resource. In this mechanism, we first build a system model and put forward its implementation process. Then, we design an encryption method used in the system model. On this basis, we discuss the function of the third party trusted platform. All of these constitute a credible mechanism of service about data resource in cloud computing. The process can be described as follows:

3.1 System Model

In cloud computing, all services provided by data resource to corresponding users are through the cloud server. At first, the user sends some data manipulation commands and requests to the cloud server, who wants to get the service of data resource. Secondly, the cloud server provides data resource services to the user through the virtual machine monitor. The virtual machine monitor plays a key role in controlling and managing the resource scheduling and service process. However, the services of data resource are usually faced with many security threats under the control and management methods. Some hackers or illegal users always want to get all kinds of information about data resource and destroy the system through a variety of ways. In order to achieve certain ulterior purpose, the hackers (or illegal users) usually use the following methods: create a large number of illegal data files, falsify the data resource, steal data, and send a large number of waste data. All these methods that the hackers used are related to the operation about data resource. In the face of a series of security problems in cloud computing, we need to construct the third party trusted platform (TTP) in cloud computing, which is used to enhance the security of service of data resource. Therefore, the system model is shown in Figure 1.

In this system model, the user is only responsible for providing the operation application to the cloud server. And the cloud server can provide the necessary data resource service according to user's requirement, such as modify, add, delete, insert and search. In the model, we suppose the cloud server contains all the data resource which is required by user and the information transmission is followed SSL (Secure socket layer) or TLS (Transport later security) protocols among the cloud service, the users and the third party trusted platform. The implementation processes can be described as follows:

Step 1: The user first encrypts a data file F by using a symmetric key K_D. Then, the encrypted file $K_D(F)$ is sent to the cloud server and the third party trusted platform.

Step 2: The symmetric key K_D is encrypted by using a public key K_P, firstly. Then, the private key K_S is signed by user. At last, the encrypted symmetric key $K_P(K_D)$ and the signed private key K_S are sent to the cloud server and third-party trusted platform by SSL or TLS.

Step 3: The cloud server will verify its identity after it received the private key K_S, which is sent by the user. If the authentication between the user and the cloud server is successful, the cloud server will receive the encrypted file $K_D(F)$ and the encrypted symmetric key $K_P(K_D)$. After that, the cloud server decodes the encrypted symmetric key $K_P(K_D)$ by the private key K_S and get a data file F^*. If the authentication is not successful, it shows error, go to Step 11.

Step 4: The cloud server encrypts the data file F^* with a symmetric key K_M, and then send encrypted file $K_M(F^*)$ to the third party trusted platform.

Step 5: The cloud server will encrypt the symmetric key K_M by using a public key K_{pc}, and then send the encrypted file $K_{pc}(K_M)$ to third party trusted platform by SSL or TLS.

Step 6: The third party trusted platform will apply for the private key K_{ps} to the cloud server after he receives the $K_{pc}(K_M)$.

Step 7: After the cloud server receives the application from the third party trusted platform, it will sign the private key K_{ps} and sends it to the third party trusted platform by SSL or TLS.

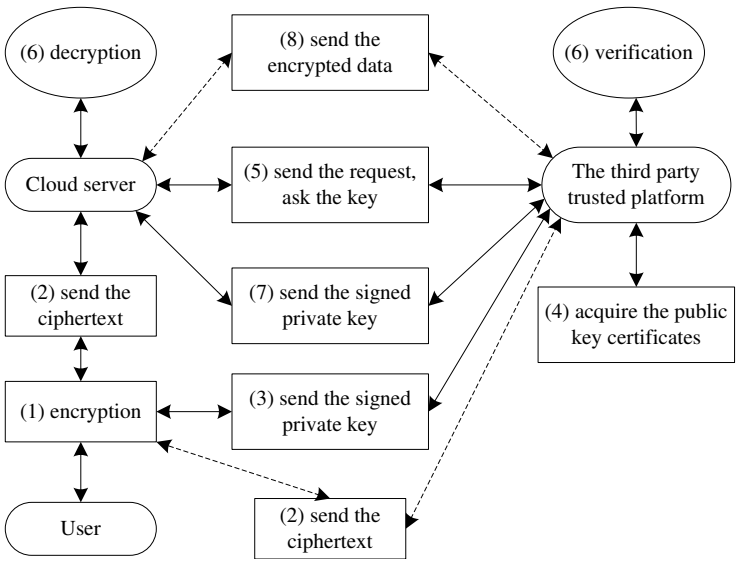

Figure 1: The system model of the credible mechanism of service about data resource

Step 8: The third party trusted platform will verify its identity after he receives the signature private key K_s. If the user authentication is successful, the third party trusted platform will decrypt the encrypted symmetric key $K_P(K_D)$ and get the symmetric key K_D. Then, the third party trusted platform will decrypt the encrypted file $K_D(F)$ and get a data file F by using the symmetric key K_D. If the authentication is not successful, it shows error and goes to Step 11.

Step 9: The third party trusted platform will verify the identity of the private key after it receives the signature private key K_{ps}, If the authentication about the cloud server is successful, the third party trusted platform will decrypt the received encryption file $K_{pc}(K_M)$ and get the symmetric key K_M. Then, it will decrypt the encrypted file $K_M(F^*)$ by using the symmetric key K_M and get the data file F^{**}, which is received from the cloud server. If the authentication is not successful, it shows error and goes to Step 11.

Step 10: The third-party trusted platform will verify whether F'' and F^{**} is uniform or not. If the two data files are same, it shows that the communication service between the users and the cloud server is credible. If the two data files are not same, it shows that the communication service between the users and the cloud server is not credible.

Step 11: End.

3.2 Encryption Method

In the credible mechanism of service for data resource, two kinds of different encryption methods are used. One is the symmetric encryption method and the other is the asymmetric encryption. In the symmetric encryption method, the *AES* Standard Advanced (Encryption) is used for encryption. The Standard is also named as the *Rijndael* encryption method, which belongs to a block encryption method. The encryption process is carried out in a 4×4 matrix of bytes and this matrix in cryptography theory is called "a state". The initial value is a plaintext block and the encryption cycle of the *AES* contains four operations: namely *AddRoundKey*, *SubBytes*, *ShiftRows* and *MixColumns*. The *AddRoundKey* operation is to make *XOR* operation for each byte in the matrix with the second round of the secret key (round key). And each sub key is generated by using the key generation scheme. The *SubBytes* operation is to replace each byte to the corresponding byte by using a lookup table, which is mainly through a nonlinear replacement function. The *ShiftRows* operation is to mix each column four bytes by using linear transformations. And the *MixColumns* operation will be omitted and replace by another *MixColumns* operation in the last encrypted loop.

In the asymmetric encryption algorithm, each entity (such as: user, cloud server *etc.*), generates a pair of keys $\langle U_k, V_k \rangle$, where U_k denotes the public key of entity U, V_k denotes the private key. In the asymmetric encryption algorithm, we will widen the *RSA* scheme to a scheme that employs the general linear group of order h with values selected randomly from the ring of integer $mod(n)$ where n is a product of two large prime numbers. The integer is coprime with n form a group under multiplication $mod(n)$ of order $g(n)$, inverse square matrices of rank h on the ring of integer $mod(n)$ will generate a group of order to this group, and this is unknown in the general scheme. But, in the general scheme where n is a product of two distinct prime numbers we can find the order of this group by the following theorem:

Theorem 1. *Assume that $n = p \times q$ is the product of two large prime numbers, and suppose that* g *is the general*

linear group of $h \times h$ matrices over Z_n. Then $g = (p^h - p^0)(p^h - p^1)\cdots(p^h - p^{h-1}) + (q^h - q^0)(q^h - q^1)\cdots(q^h - q^{h-1})$.

Proof. Each matrix $x \in g$ decreased to two matrices x_p and x_q such that x_p and x_q are $h \times h$ matrices on the members z_p and z_q such that $x_p = xmodp$, $x_q = xmodq$. Actually, a mapping: $f : g(n,h) \to g(p,h) \oplus g(q,h)$, is the ring identical of a two rings. □

In the asymmetric encryption algorithm, The whole processes include three phases, namely the key generation phase, the encryption phase and the decryption phase. Each phase is described as follows, respectively.

1) The key generation phase:

   Step 1: Entity U randomly and secretly chooses two large primes p and q, and compute $n = p \times q$.

   Step 2: Entity U computes $\psi(n) = (p-1)(q-1)$.

   Step 3: Entity U computes $g(n,h) = (p^h - p^0)(p^h - p^1)\cdots(p^h - p^{h-1}) + (q^h - q^0)(q^h - q^1)\cdots(q^h - q^{h-1})$.

   Step 4: entity U selects a random integer r, such as $1 < r < n$ and $gcd(r, \psi(n)) = 1$ and $gcd(r, g(n,h)) = 1$ (where r should be a small integer)

   Step 5: Entity U computes e such as $r \cdot e \equiv 1 mod \psi(n)$ and $1 < e < \psi(n)$.

   Step 6: Entity U computes d such as $d \cdot e \equiv 1 mod g(n,h)$ and $1 < e < g(n,h)$.

   Step 7: Entity U gets the public key $U_k \leftarrow (e,n)$

   Step 8: Entity U gets the private key $V_k \leftarrow (r,d,n)$

2) The encryption phase:
   Suppose entity M needs to send message m to entity U (represents m as an integer in the range of $0 < m < n$).

   Step 1: Entity U should send his public key to entity M.

   Step 2: Entity M will encrypt m as $c = ((m^e mod n)^e mod n)$.

   Step 3: Entity M will send c to entity U.

3) The decryption phase:

   Step 1: Entity U will decrypt the received message as: $m = ((c^r mod n)^d mod n)$.

3.3 The Third Party Trusted Platform

The main functions of the trusted third party platform include: (1) Receiving the private key of user. (2) Possessing the public key certificate which is authorized by the user. (3) Sending a private key to the cloud server. (4) Verifying the credibility of data that the cloud server receives or transmits. By using the third party trusted platform, we can get that if the communication service between the users and the cloud server is credible or not. Therefore, the section will describe the four aspect functions.

1) Receiving the private key of user:
   In order to hold the private key of each user in cloud computing, the third party trusted platform needs to constantly modify the database of the cloud user. All important information for each user are included in the database of the cloud user, such as the private key, the digital certificate of user, the key and the hash value of the cloud server.

2) Possessing the public key certificate which is authorized by the user:
   Once the third party trusted platform received the encrypted private key sent from the user, it possesses the public key certificate authorized by the user. In order to obtain the public key certificate, the user must use the private key to sign and then encrypt the signed information. On the basis of these steps, the user will send the signed and encrypted information to the third party trusted platform. For example, $E_{v_k \to user}\langle E_{U_k \to TTP}(K_s)\rangle$, where U_k denotes the public key of the user, v_k the private key of the user. Therefore, if the third party trusted platform wants to verify the user's identity, it needs to decrypt the signed and encrypted information, firstly. Then, it can verify the user's identity. The whole verification processes can be described as follows: $D_{U_k \to user}(E_{v_k \to user}\langle E_{U_k \to TTP}(K_s)\rangle) = E_{U_k \to TTP}(K_s)$.

3) Sending the private key to the cloud server:
   Before providing the service for the user, the trusted third party platform needs to verify the identity of the cloud server. The basic processes can be described as follows: $D_{U_k \to user}(E_{v_k \to user}(F_{K_D}) = H(M_i))$, where H is a cryptographic hash function. The main function of H is to encrypt the data blocks m_i of the data file F and generate a 160 bit hash value. Once the identity of the cloud server is authenticated, the third party trusted platform will take out the corresponding private key of the user from its own database and encrypt the private key by using the *RAS* encryption method. After that, the encryption data information is sent to the cloud server.

4) Verifying the creditability of the received or sent data:
   If the third party trusted platform receives the signature private key K_s, it will verify the identity of the user. If the authentication about the identity of the user is successful, it will decrypt the encrypted symmetric key $K_P(K_D)$ and get the symmetric key K_D. Then, it will decrypt the encrypted file $K_D(F)$ and get a data file F^{**} by using the symmetric key K_D. If it receives the signature private key K_{ps}, it will verify the identity of the cloud server. If the authentication about the identity of the cloud server is successful, it will decrypt the received encryption file $K_{pc}(K_M)$ and get the symmetric key K_M. Then, it will decrypt the encrypted file $K_M(F^*)$ by using the

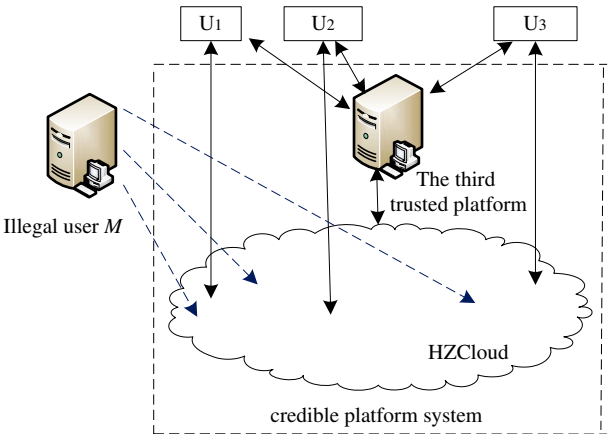

Figure 2: The overall framework of experiment

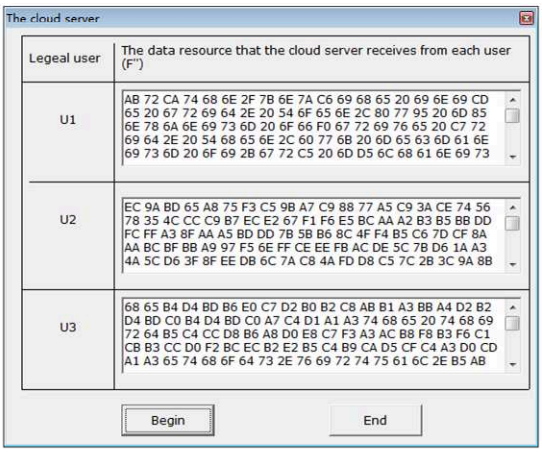

Figure 3: The data resource that the cloud server receives from each user

symmetric key K_M and get the data file F^{**}. At last, the third-party trusted platform will verify whether F'' and F^{**} is uniform or not. If the two data files are same, it shows that the communication service between the users and the cloud server is credible. Otherwise, it shows that the communication service between the users and the cloud server is incredible.

4 Experiment and Result Analysis

In order to verify the validity of this mechanism, we first carried out a series of experiments. On this basis, the experimental results and the advantages are analyzed. The whole processes are described as follows.

4.1 Experiment

In our experiments, we first constitute a credible platform system by using our proposed credible mechanism of service about data resource which is based on *HZCloud* cloud computing environment. In the credible platform system, it includes the cloud server, the third party trusted. Moreover, we built three legal users (namely, U_i(i=1, 2, 3)) and each legal user can use a different virtual machine which is respectively virtualized from the cloud server. Each legal user can submit some application to the cloud server and can get corresponding service of data resource. At the same time, there is an illegal user M who wants to steal the sent data resource. The overall framework of experiment is shown in Figure 2.

By using the credible platform system, we can get the state that the cloud server receives data resource from each user in the third trusted platform. The data resource that the cloud server receives from each user are shown in Figure 3, respectively.

Moreover, we can also get the state that the third trusted platform receives data resource from each user.

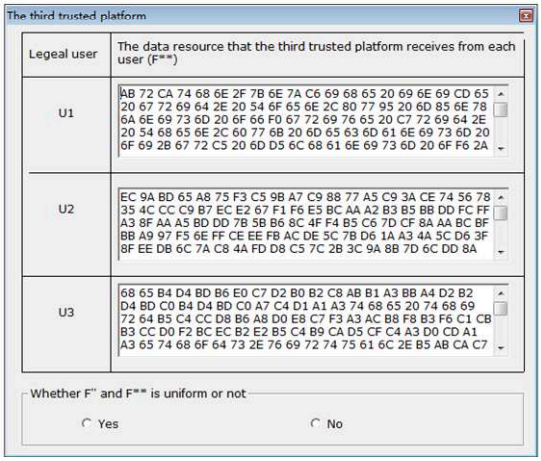

Figure 4: The data resource that the third trusted platform receives from each user

The data resource that the third trusted platform receives from each user are shown in Figure 4, respectively.

In addition, we also get the data resource that the illegal user M steals. The result is shown as Figure 5.

4.2 Result Analysis

Comparing the "The data resource that the cloud server receives from each user" column of Figure 3 with the "The data resource that the third trusted platform receives from each user" column of Figure 4, we will find that the data resource that the cloud server receives from each user is the same as the data resource that the third trusted platform receives from each user, respectively. In addition, we can also find the data resource that the illegal user M receives from each user all are digital gibberish. These show that the cloud server can efficiently receives the data resource from each user and the illegal user M cannot decrypt the encrypted data resource although he

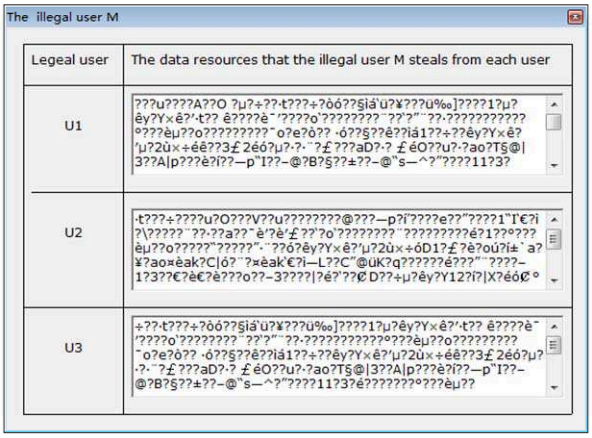

Figure 5: The data resource that the illegal user M steals from each user

can steals data resource from each user. The main reason that these situations generate is that our proposed encryption method is used.

4.3 Advantage Analysis

1) The key range of the described asymmetric encryption algorithm in our paper is considerable. It means that it can be large enough to use by matrices of high level of ranks. The key range for instance in the *RSA* scheme is $\psi(n) = (p-1)(q-1)$. But, in our described asymmetric encryption algorithm, the key range is of length $g(n,h)$. So, the differences between the two ranges are obvious.

2) The described asymmetric encryption algorithm in our paper can be used with Hill cipher method to obtain more intractable encryption system. Moreover, the described asymmetric encryption algorithm can be employed using a subgroup instead of a full value of $g(n,h)$, since the $gcd(r, g(n,h)) = 1$. Thus, the described asymmetric encryption algorithm in our paper will give more flexibility to entity to use more than one technique.

3) The intractability of the integer factoring of the modulus n in the described asymmetric encryption algorithm stays as same as in the *RSA* scheme.

From the above result analysis and the above advantage analysis, we can get that the data resource service between the users and the cloud server is credible.

5 Conclusion

In cloud computing, the access of user is becoming more and more frequently own to the scale growth of the data resource. The network attacks that users and cloud server confront are also becoming more and more frequently. Under the situation, the security protection of data resource in cloud computing becomes very difficult. The traditional network security methods can play a certain role in maintenance the security of data resource. However, these traditional network security methods are also facing many difficulties in the face of virtualized computing environment. In this situation, we propose a credible mechanism of service for data resource in cloud computing. In order to verify the feasibility of the mechanism, a series of experiments have been done. The experimental results show that it is feasible to ensure the security of service about data resource in cloud computing.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (no. 61472112). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] Y. A. A. S. Aldeen, M. Salleh, and Y. Aljeroudi, "An innovative privacy preserving technique for incremental datasets on cloud computing," *Journal of Biomedical Informatics*, vol. 62, pp. 107–116, 2016.

[2] J. Arshad, P. Townend, and J. Xu, "A novel intrusion severity analysis approach for clouds," *Future Generation Computer Systems*, vol. 29, pp. 416–428, 2013.

[3] B. Balusamy, P. V. Krishna, G. S. T. Arasi, and V. Chang, "A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System," *International Journal of Network Security*, vol. 19, no. 4, pp. 559–572, 2017.

[4] Z. Cao, C. Mao, and L. Liu, "Analysis of One Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.

[5] T. Y. Chang, M. S. Hwang, and W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences* , vol. 181, pp. 217–226, 2011.

[6] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *Computers and security*, vol. 42, pp. 151–164, 2014.

[7] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommunications Policy*, vol. 37, pp. 372–386, 2013.

[8] L. Liu, W. Kong, Z. Cao, and J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, Vol. 6, No. 2, pp. 110–115, 2017.

[9] M. Mackay, T. Baker, and A. Al-Yasiri, "Security-oriented cloud computing platform for critical infrastructures," *Computer Law and Security Review*, vol. 28, pp. 679–686, 2012.
[10] G. Manogaran, C. Thota, and M. V. Kumar, "Metaclouddatastorage architecture for big data security in cloud computing," *Procedia Computer Science*, vol. 87, pp. 129–133, 2016.
[11] Y. Ming and Y. Wang,"On the security of three public auditing schemes in cloud computing," *International Journal of Network Security* , vol. 17, No. 6 pp. 795–802, 2015.
[12] A. Mosa, H. M. El-Bakry, S. M. Abd El-Razek, S. Q. Hasan, "A proposed E-government framework based on cloud service architecture," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 93–104, 2016.
[13] R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, vol. 48, pp. 204–209, 2015.
[14] H. Rasheed, "Data and infrastructure security auditing in cloud computing environments," *International Journal of Information Management*, vol. 34, no. 3, pp. 364–368, 2014.
[15] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers and Electrical Engineering*, vol. 39, pp. 47–54, 2013.
[16] A. P. Singh and S. K. Pasupuleti, "Optimized public auditing and data dynamics for data storage security in cloud computing," *Procedia Computer Science*, vol. 93, pp. 751–759, 2016.
[17] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.
[18] R. Trapero, J. Modic, M. Stopar, A. Taha, and N. Suri, "A novel approach to manage cloud security SLA incidents," *Future Generation Computer Systems*, vol. 72, pp. 193-205, 2017.
[19] N. Vurukonda and B. T. Rao, "A study on data storage security issues in cloud computing," *Procedia Computer Science*, vol. 92, pp. 128–135, 2016.
[20] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371–386, 2014.
[21] D. Wu, B. Yang, and R. Wang, "Scalable privacy-preserving big data aggregation mechanism," *Digital Communications and Networks*, vol. 2, no. 3, pp. 122–129, 2016.

Biography

Yunfa Li is a Ph.D.and associate professor in school of Computer Science and Technology at Hangzhou Dianzi University. His research interests include cloud computing, cluster computing, grid computing, big data and system security. Contact him at yunfali@hdu.edu.cn.

Yangyang Shen is a postgraduate in school of Computer Science and Technology at Hangzhou Dianzi University. His research interests include cloud computing, big data and system security. Contact him at 2644294165@qq.com.

Mingyi Li is a postgraduate in school of Computer Science and Technology at Hangzhou Dianzi University. His research interests include cloud computing, big data and system security. Contact him at 952921628@qq.com.