Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

Data Security Protection in Cloud Computing by using Encryption

Asst. Lec. Ghassan Sabeeh Mahmood

Computer Science Department, College of Science, University of Diyala, Iraq

ghassan@sciences.uodiyala.edu.iq

Abstract

Cloud computing is a paradigm for offer information technology services on the Internet, such as hardware, software, networking and also the storage can be accessed anywhere at any time on a pay-per-use basis. However, storing private data onto servers of the cloud is a challenging matter. Therefore, cryptography technique and authentication are used in this model to ensure confidentiality and proper access control of sensitive data. Therefore, in this paper I proposed a model to protect data in cloud computing. In this model the algorithm of the Rivest-Shamir- Adleman (RSA) is applied to the private data. Furthermore, the protocol of Challenge-Handshake -Authentication-Protocol (CHAP) is used to improve the security of the authentication as well. The results show this model is secure and practical.

Keywords: Cloud Computing, Security, Encryption, Authentication.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 4, September 2017
ISSN 1992 – 0849

حماية أمنية البيانات في الحوسبة السحابية باستخدام التشفير

م.م غسان صبيح محمود

قسم علوم الحاسوب، كلية العلوم، جامعة ديالى، العراق

ghassan@sciences.uodiyala.edu.iq

الملخص:

سحابة الحوسبة هي نموذج لتقديم خدمات تكنولوجيا المعلومات على شبكة الإنترنت، مثل الأجهزة والبرمجيات، والشبكات، وأيضا التخزين يمكن الوصول إليه في أي مكان وفي أي وقت على أساس الدفع-لكل-استخدام. ومع ذلك، تخزين البيانات الخاصة على ملقمات سحابة الحوسبة هي مسألة صعبة. ولذلك، تستخدم تقنيات التشفير والمصادقة في هذا النموذج لضمان السرية والتحكم بالوصول السليم للبيانات الحساسة. لذا، اقترحت في هذه الورقة نموذج يسمى (حماية أمن البيانات في الحوسبة السحابية باستخدام التشفير) لحماية البيانات في سحابة الحوسبة. وفي هذا النموذج يتم تطبيق خوارزمية (RSA) للبيانات الخاصة. وعلاوة على ذلك، يتم استخدام بروتوكول (CHAP) لتعزيز الأمن لخدمة المصادقة كذلك. وتبين النتائج التجريبية ان هذا النموذج ليس فقط آمن ولكن أيضا عملي.

كلمات دالة: الحوسبة السحابية، الحماية، التشفير، المصادقة.

1. Introduction

Cloud computing technology is a model for enabling network access to a shared set of computing resources (e.g., Servers, networks, applications, services, and storage) [**1**]. It has become a popular topic of research. In general, a cloud computing is another important service after electrical, gas, water and telecommunication services [**2**].

Cloud services consist of three types of services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS Cloud providers offer physical, virtual computer and extra storage networking devices. Example of IaaS includes Amazon Elastic Compute Cloud (EC2), [**3**]. PaaS, users can deploy applications over the cloud-computing infrastructure, without controlling it. Instead of supplying services, the providers offer libraries and tools to deploy the application itself. Example of PaaS the Google Apps Engine [**4**]. SaaS provides an application development service to customers either as a service on demand. Example SaaS Salesforce.com, Customer Relationship Management (CRM), Google Docs and Google Gmail. [**3**].

Cloud services can be classified according to different deployment models, public cloud, private cloud, hybrid cloud and community cloud. A public cloud which is developed by a cloud service provider, public cloud is available to all end users. A private cloud which is developed by a particular organization for their personal uses. A hybrid cloud is used to make organization scalable. Any private cloud can be extended to public cloud in a hybrid cloud. Several organizations combine to form their private cloud in a community cloud [**5**].

Move into cloud occurs because cloud computing allows users to access applications from anywhere at any time online [**6**]. Storing the data in the cloud computing offers to users the convenience of access without requiring direct knowledge the deployment and management the hardware or infrastructure. Cloud is more powerful than persona computing, however, it's bringing new security challenges. A full access to cloud computing services, results the exposure the data of users to several threats and malicious attacks [**7**].

Therefore, security is considered the key requirement for cloud as a robust and meaningful solution. These risks were motivated us to think about a solution to protect data stored in cloud computing. Therefore, data security protection model has been presented in this paper.

The rest of my paper is as follows: Section 2 contains the related works. Section 3 includes the cloud security. Section 4 defines the proposed scheme. Section 5 demonstrates the experimental results. This paper concluded in Section 6.

2. Related Works

With regard to the importance of data security in the cloud, numerous models presented to improve the reliability and efficiency in cloud computing environments.

Guojun W. And et al. Proposed a hierarchical attribute based encryption (HABE) system by merging (HIBE) system and (CP-ABE) system, to offer access and a good performance. And then, they proposed system by applying (PRE) and (LRE) to the HABE system to revoke access from users [**6**].

Joseph K. L. And et al. Proposed system with issue revocability for cloud storage. This system lets a correspondent to send an encrypted letter to a receiver. The sender just knows the individuality of the receiver. The receiver has two things to decrypt the letter. The initial is the top-secret key stored in the computer. The other is the security device that joins to the computer. If this device is missing, then the device is cancelled. This process can be completed through the cloud computing server that immediately executes algorithms to modify the existing ciphertext. The cloud computing servers can't decrypt ciphertext at any time [**8**].

Rongmao C. And et al. Proposed a model named dual server PEKS (DS-PEKS). They also defined a variant of (SPHF) denoted to as (LH, SPHF). And then, they presented a basic creation of DS, PEKS from (LH, SPHF) to show the practicability of the model. And they offer an instantiation of the framework from a decision Diffie–Hellman-based LH-SPHF [**9**].

D. Sangeetha and et al. Proposed a secure cloud computing based PHR model to share PHR among several users by using attribute-based encryption. In the proposed model, patients can encode their PHR and put them on cloud. The proposed PHR model is separated into personal domain and the public domain. To guarantee safety in a cloud, (S, KP, ABE) and (PP, DCR, ABE) algorithm are executed in the personal domain and the public domain [**10**].

3. Security of Cloud Computing

In our life data plays a significant role. It is formed from several sources such as persons, devices, etc. Therefore, we deal with an important matter, that affects all science [**11**]. Security of data and trust problem have always been the key and challenging matters in cloud [**12**]. At risk of data abused exists when many users share resources. Accordingly, the data necessity be secured to avoid this risk.

The cloud security includes three important requirements it is confidentiality, integrity and availability.

3.1 Confidentiality

Weaknesses must be checked to certify that data is protected from attacks. Consequently, security test must be finished to protect data.

3.2 Integrity

Users must worry about the integrity of data. Since confidentiality does not indicate integrity. For confidentiality purposes, data can be encrypted, however, users may not have a way to verify data integrity. Consequently, the integrity of data needs the use of the authentication.

3.3 Availability

It is the most significant matter in numerous organizations that facing the stopped as a key matter [**13**].

Consequently, to enhance the security in cloud computing the encryption algorithm and authentication model are suggested as solutions in this paper.

4. Proposed Scheme

In this work, I proposed “data security protection in cloud computing by using encryption” to protect the sensitive data in the cloud.

4.1 Sub-parameters of the proposed system

The security of the proposed system is accomplished according to following sub-parameters:

4.1.1 Authentication

It is the process of proving a user's identity. Therefore, by using the authentication the proposed system increases the rate of resistance against users unauthorized. In cloud computing model, the Challenge-Handshake-Authentication -Protocol (CHAP) is an authentication protocol used to authenticate the individuality of customers.

Challenge-Handshake-Authentication-Protocol confirms the individuality of the client by using a three method:

When the client requests a service, the Service Provider Authentication sends a (challenge) message to the client, after that.

Responds the client with a value that is calculated by using a hash function. The authenticator confirms from response values, If the values Are identical, the authentication it will be login, if not it should end the connection (see figure 1)** [14]**.

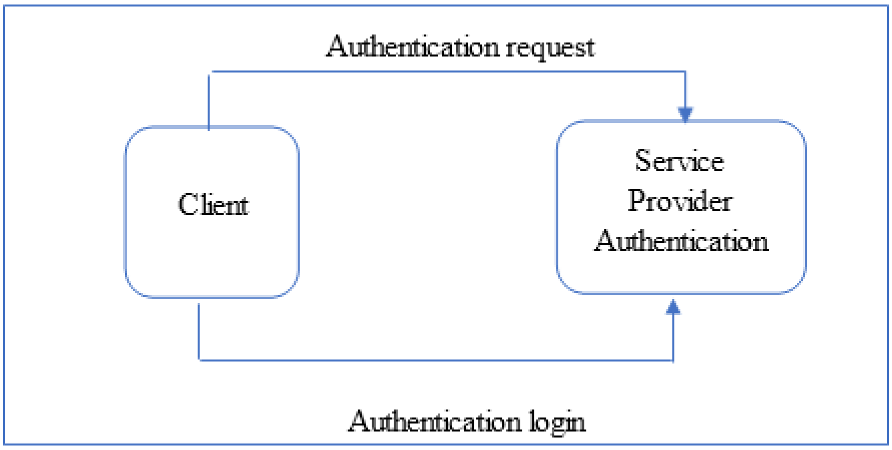

Figure 1: Implementation of CHAP

In the proposed model, I use Challenge-Handshake-Authentication-Protocol (CHAP) for authentication.

4.2.1 Cryptography

It is the most public solution to guarantee data protection in the cloud. [**15**]. consequently, in the proposed model Rivest-Shamir- Adleman (RSA) algorithm applied to the sensitive data. Furthermore, I used a protocol (Challenge- Handshake -Authentication -Protocol) to improve the security of the authentication.

4.2 Data Storage Process Algorithm:

- The user sends the authentication request to the Cloud Service Provider.

- Cloud Service Provider verifies the authorization using CHAP and sends the acknowledgement back to the user.
- User encrypts the sensitive data (S) by using RSA algorithm.
- Send the data to the cloud by using the function: Send _ to _ cloud (S'): It permits to send the encrypted file (S') in cloud storage.

4.3 Data Retrieval Process Algorithm:

When the user downloads the data from the cloud, it received in the encrypted form. To use the data, I apply the data retrieval process algorithm by using RSA algorithm.

5. EXPERIMENTAL RESULTS

In this paper, I propose a data security protection in the cloud using encryption and authentication module to protect data. The proposed method implemented in Matlab. The results in this section highlight the time of execution in send and receive data with different sizes and response time for cryptography (see table 1).

Table 1: Execution time and Cryptographic performance

Block size (KB)	Response time (s)		Execution time (s)	
	Encryption performance	Decryption performance	Send data	Receive data
256	0.3243	0.6689	0,5152	0,8451
512	0.6992	0.7739	0,8054	0,9835

6. *CONCLUTION*

In this paper, I proposed a solution to cloud storage security problems in terms of confidentiality, availability and integrity to protect the data stored in the cloud. In this model, the RSA algorithm is applied to the sensitive data. Furthermore, I used authentication protocol to improve the security of the authentication. The stored data use encryption and only the authorized user can access the data. Even if unauthorized users reach the data, they cannot decrypt these data. In the future, other algorithms can be used to protect the data stored in cloud computing.

References

[1] Paulo A., Leal R., Danielo G.¸ Alves G. and Jos´e Neuman de S., “Elasticity in cloud computing- a survey”, Annals of telecommunications, Vol 70, (2015),No.7., pp. 289–309.

[2] Xi L. and Jun L., "Distributed Management Method in Cloud -Computing Environment", International Journal of Hybrid Information Technology, Vol. 9, (2016), No. 5, pp. 371-380.

[3] , Jesus C. and Javier G. Blas, "Introduction to cloud computing-platforms and solutions", Cluster Computing, Vol.17, (2014), No.4., pp. 1225–1229.

[4] Hfer, C.N., Karagianni, G., "Cloud computing services- taxonomy and comparison", Journal of Internet Services and Applications, Vol.2, (2011), No.2, pp. 81–94.

[5] Sean C. and Kevin C., "Cloud Computing -Security", International Journal of Ambient Computing and Intelligence, Vol.3, (2011), No.1, pp. 14-19.

[6] G. Wang, Q. Liu, J. Wu and M. Guo," Hierarchical -attribute- encryption user revocation for sharing data in -cloud servers", Computers and security, Vol.3, (2011), pp. 320–331.

[7] 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 & security, Vol 4, (2 0 1 4), pp. 151–164,.

[8] Joseph K. Liu, K. Liang, W. Susilo, J. Liu and Yang X. "Data security protection for cloud -Storage System", IEEE Transaction Computers, Vol.65, (2016), No.6, pp. 1992 - 2004.

[9] R. Chen, Yi Mu, G. Yang, F. Guo, and X. Wang, "Dual Server Public Key Encryption- with Keyword Search", IEEE transaction on information forensics and security, Vol. 11,(2016), No. 4., pp. 789 – 798.

[10] D. S. and V. Vaideh, "A secure cloud based- Personal Health Record framework for a multi -owner environment ", Annals of Telecommunications, (2016), pp. 95–104.

[11] H. Shirvani1 and H. Vahdat-Nejad, "storing shared document that are customized by users on cloud", Computing, (2016), pp. 1137–1151.

[12] X. Lei, X. Liao, X. Ma and L. Feng, "Securely and efficiently perform large matrix rank decomposition computation via cloud", Cluster Computing, Vol.18, (2015), No.2., pp. 989–997.

[13] Muhammad Y. S., Asif I., Zahid M. and AtaUllah G., "Analysis of Classical Encryption Techniques in Cloud Computing", Tsinghua Science and Technology, Vol.21, (2016), No.1, pp. 10 2-1 13.

[14] https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol.

Moussa O., Severine M., Herve C., Steven F. and Eric D., "The next frontier for security research in cloud ", Cloud Computing, pp., 2015.