IBIMA Publishing
Journal of Cloud Computing
http://www.ibimapublishing.com/journals/JCC/jcc.html
Vol. 2016 (2016), Article ID 179794, 6 pages
DOI: 10.5171/2016.179794

Research Article

Using Security Features for Cloud Computing Based on New Symmetric Key Algorithm

Saeed Q. Al-Khalidi Al-Maliki[1] and Fahad Alfifi[2]

[1]King Khalid University, Abha, K.S.A

[2]Robert Morris University, Pittsburgh, U.S.A

Correspondence should be addressed to: Saeed Q. Al-Khalidi Al-Maliki; salkhalidi@yahoo.com

Received date: 22 March 2014; Accepted date: 28 June 2015; Published date: 13 July 2016

Abstract

Cloud computing platforms deliver critical business applications in large part because of sales commitments to security and privacy. With the help of cloud computing, large pools of resources can be connected via private or public networks to provide dynamically scalable infrastructures for application, data and file storage. Additionally, the costs of computing, application hosting, content storage and delivery can be significantly reduced. However, problems arise with cloud computing concerning data privacy, security and authenticity. Hence, our research paper presents an efficient method for providing data-storage security in cloud computing using a new simple symmetric key algorithm. This algorithm includes such important security services as key generation, encryption and decryption that are provided in cloud computing systems. The main scope of this paper is to solve the security issues in both cloud providers and cloud consumers using new cryptography methods.

Keywords: Cloud computing, simple symmetric key algorithm, Encryption / Decryption.

Introduction

Cloud computing has become one of the most important new technologies in recent times, integrating previous computing power technologies to help organisations improve and develop their quality of work (Hayes, 2008). Cloud computing is a general term that can be used in various contexts and with different meanings. However, the most common definitions agree that cloud computing is distributed among computing components over the Internet providing three different types of services. First, the Software-as-a-Service (SaaS) model offers services as applications to the consumer using standardised interfaces. The consumer can only control some of the user-specific application configuration settings (Mithila and Kumar, 2011). Second, the Platform-as-a-Service (PaaS) model offers services as operation and development platforms to the consumer. In these instances, the consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but does have control over the deployed applications and possibly over the application-hosting environment configurations (Mithila and Kumar, 2011). Finally, the Infrastructure-as-a-Service (IaaS) offers infrastructure resources as a service, such as raw data storage,

Cite this Article as: Saeed Q. Al-Khalidi Al-Maliki and Fahad Alfifi (2016), "Using Security Features for

processing power and network capacity. The consumer does not manage or control the underlying cloud infrastructure but does have control over operating systems, storage, deployed applications, and possibly limited control of select networking components (Mithila and Kumar, 2011). The National Institute of Standards and Technology (NIST, 2012) noted cloud computing as an innovation that allows large groups of customers to access a pool of on-demand, pay-as-you-go computing resources, such as networks, storage, applications, and services.

Furthermore, users and organisations can use cloud computing services by subscribing through many different companies which provide three levels of cloud types: public, private or hybrid. Cloud computing provides many advantages to organisations at all levels, such as lowering costs and improving service quality, simplifying IT complexity, improving IT quality and allowing IT managers to focus on the essential mission, objectives and processes. Cloud computing technology provides unlimited storage capacity, increased data reliability and flexibility (Workday, 2011). Cloud computing is the key driving force in many small, medium and large-sized companies and, as many potential cloud users seek the services of cloud computing, the major concern has become the security of their data in the cloud. Securing data is always of vital importance, and, because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Encryption is the conversion of data into coding, called ciphertext, which cannot be read or modified by unauthorised users. There are two main types of encryption techniques: symmetric-key and public-key encryption (Goldreich, 2004). In this paper, we attempt to demystify data-storage security in a private cloud computing environment and clarify issues from a security perspective by using a new simple symmetric-key algorithm. In this algorithm, some important security services are included, such as key generation, encryption and decryption as provided in cloud computing systems. Moreover, in this paper, we have proposed a new level of data security solution by using the Reverse Caesar cipher algorithm with encryption using ASCII full 256 characters; consequently, compared to other encryption methods, our new encryption algorithm is very secure. The main goal of this paper is to solve security issues for both cloud providers and cloud consumers using new cryptography methods.

Literature Review

Cloud computing is an upcoming paradigm that offers tremendous advantages in terms of economics, such as reduced time to market, flexible computing capabilities and limitless computing power. To use the full potential of cloud computing, data are transferred, processed and stored by external cloud providers. However, data owners are very sceptical of placing their data outside their own control sphere (Mithila and Kumar, 2011). The proposed solutions for network security include such concepts as cryptography whereupon the distribution of keys is done. Encryption and key generation are a vital tool for preventing threats to data sharing and preserving data integrity, so we are focusing on enhancing security by enhancing the level of encryption in the network. In their research, Kuppuswamy and Al-Khalidi (2012) proposed selecting any number and calculating the inverse of the selected integer by using modular 37. This paper aims to propose an efficient method for providing data-storage security in cloud computing using the RSA algorithm. This algorithm includes some important security services such as key generation, encryption and decryption as they are provided in a cloud computing system (Sunitha and Prashanth, 2013).

The main scope of this paper is to solve security issues facing both cloud providers and cloud consumers using cryptography encryption methods. Understanding a cipher text is complicated compared to other methods (Subhasri and Padmapriya, 2013). Singla and Singh (2013) described the cloud as being the most vulnerable next-generation architecture consisting of two major design elements: the Cloud Service Provider (CSP) and the client. Even though cloud computing is promising and efficient; there are many challenges in terms of data privacy and security. This

paper explores the security of data at rest, as well as the security of data while moving (Subhasri and Padmapriya, 2013). Furthermore, Chavan and Bangare (2013) discussed a Customer Relational Management (CRM) system, a service using the RC5 algorithm, which is a block cipher notable for its simplicity, designed by Ronald Rivest in 1994; RC stands for "Rivest Cipher," or, alternatively, "Ron's Code" (Chavan and Bangare, 2013; Kuppuswamy and Al-Khalidi, 2012). In the proposed system, the party using cloud storage services must encrypt the data before sending it to the cloud while the service provider responsible for the encryption/decryption of the user's data must then delete the data once the encryption/decryption process is completed.

Problem Statement

Cloud computing security is a very critical issue, where data can be in different physical locations at any data centre across the world network. This new technology structure leads to serious issues regarding security, such as authentication, data integrity, account or service hijacking, hypervisor vulnerabilities, data loss or leakage and confidentiality (Suthar, et al., 2012). In addition, the Cloud Security Alliance (CSA) (2013) identified data breaches as one of the top nine cloud computing threats for the year 2013, wherein a hacker is able to use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. Despite this knowledge, it is not clear today how to coordinate appropriate and efficient incident responses without impacting the continuity of operations for other customers or without violating laws and contractual agreements. In addition, the speed with which incidents must be resolved becomes much greater. Since researchers of cloud computing security are giving less attention to selecting and using the right encryption and encoding algorithms, this paper proposes implementing secure developed security algorithms that could provide cloud storage higher performance and security as a replacement for the existing private cloud storage system.

Proposed Work

A private cloud is one in which the services and infrastructure are maintained on a private network. These types of clouds offer the greatest level of security and control, but they require the company to purchase and maintain all the software and infrastructure, which reduces the cost savings.

We know that a user ID typically consists of letters from A to Z and numbers between 0-9. Here, in the new symmetric key algorithm, we introduce synthetic data, based on the user ID. Normally, the synthetic data value consists of an equivalent value of alphabets and numbers. Alphabet value A is assigned as integer number 1 and B=2 and so on. Next, we consider an integer value 0 assigned as 27 and 1=28…9=36; in addition, the space value is considered as an integer, number 37.

- Key generation method:

- Select any natural number as n

- Find the inverse of the number using modulo 37(key 1), as k

- Again, select any negative number (for making secured key) n1

- Find the inverse of negative number using modulo 37(key 2) k1

- Encryption method:

- Assign synthetic value for user ID

- Multiply synthetic value with random selected natural number

- Calculate with modulo 37

- Again, select random negative number and multiply it

- Again, calculate with modulo 37 CT = (PT* n*n1) mod 37

- Decryption method:

- Multiply received text with key1 & key2

- Calculate with modulo 37

- Remainder is Revealed Text or Plain Text PT = $(CT*n^{-1}*n1^{-1})$ mod 1

Implementation

An encryption system is one in which the sender and the receiver of a message share a single, common key that is used to encrypt and decrypt the message. This is in contrast to public-key cryptology, which utilises two keys—a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES), however, the drawback of DES encryption and decryption is that key generation timing is very high. The implementation of the proposed algorithm will produce an effective encryption/decryption method suitable for all applications.

Key Generation

- We are selecting random integer number n=3
- Then inverse of 3=25(verification 3x25 mod 37=1); So, Key1=25
- Again, we are selecting random negative number n1= -8
- Then inverse of –8 = 23(verify -8 x 23= -184 mod 37 = 1) So, Key2 =23

Encryption Method

For encryption purposes, we are arranging text in a sequence table and selecting random encryption; key1 is assumed here as n=3 and key2 n1= -8, Then, we are using modulation 37 with plain text. The calculation of encrypted text is described in the following table via a calculated message known as a cipher text or encrypted text.

Table 1: Encryption Table

Text	Integer Value	CT=(M*n) mod 37	CT=(CT*n1) mod 37	Encrypted text
S	19	20	25	Y
A	1	3	13	M
U	21	26	14	N
D	4	12	15	O
I	9	27	6	F

Decryption Method

For encryption purposes, we are arranging text in a sequence table and selecting random encryption; key1 is assumed here as n=3 and key2 n1= -8, Then we are using modulation 37 with plain text. The calculation of encrypted text is described in the following table via a calculated message known as a cipher text or encrypted text.

Table 2: Decryption Table

Text	Integer Value	PT=(CT*25*23) mod 37	Encrypted text
Y	25	19	S
M	13	1	A
N	14	21	U
O	15	4	D
F	6	9	I

Discussion of Results

A private cloud service offers a number of advantages that make it a more viable cloud solution over a public cloud service option and, consequently, our proposed symmetric key algorithm is more suitable for private cloud services. Dedicated to a single organisation, the hardware, data storage, and network can be designed to assure high levels of security that cannot be accessed by other clients in the same data centre. To be clear, this is not to say that a public cloud service is not secure. Rather, certain companies may feel data are more secure by having the data reside in-house. Another reason that a private cloud may be desirable has to do with a country's regulatory issues. In certain countries, the data centre hosting a public cloud service must also reside within the country where its users reside. Thus, when there is no public cloud option that can be provided within a country, a private cloud may be the only option that can be used.

When the private cloud is deployed inside the firewall on an organisation's intranet, transfer rates are dramatically increased versus using the Internet. In addition, there is no worry of slow page access times which may occur when using a public cloud service. Hardware performance, network performance, and storage performance can be specified and customised in the private cloud since it is owned by the company.

Conclusion

Data security has become the most important issue for cloud computing security. Though many solutions have been proposed, many of them only consider the 26 letters of the alphabet. The cloud security protocol depends on the way a cloud service provider (CSP) allows its client to register with the cloud network. In our survey, we analyse how security is provided to the data at rest, i.e., encryption is done by the cloud service provider. This study of a symmetric key algorithm effectively and efficiently recognises the security laws concerning secure cloud application management, proposing the separation of secure storage and independent secure services into different cloud service providers. Hence, the storage of the data takes place at one cloud server and the security service is provided by another server. Thus, a user sends unencrypted data from the secure cloud service providers to the independent secure cloud service system; thereafter, the independent secure cloud service encrypted data are sent to the secure storage cloud system. Data decryption in the cloud is the exactly the reverse process of the encryption system. In this system, the independent secure cloud service uses a simple symmetric encryption/decryption algorithm. This system will be beneficial for the end user and will enhance data security in cloud computing.

References

1. Chavan, S. K. and Bangare, M. L., 2013. Secure CRM Cloud Service using RC5 Algorithm. *International Journal of Computer Trends and Technology*, 4 (3), 325-330.

2. Goldreich, O., 2004. *Foundations of Cryptography. Volume II, Basic Applications.* Cambridge: Cambridge University Press.

3. Hayes, B., 2008. Cloud Computing. *Communications of the ACM,* Vol. 51, pp.9-11.

4. Mithila S., and Kumar P., 2011. Data Security through Confidentiality in Cloud Computing Environment. *(IJCSIT) International Journal of Computer Science and Information Technologies*, 2(5), 1836-1840.

5. NIST, 2012. *Institute of Standards and Technology (NIST),* [online] Available at:, http://csrc.nist.gov/publications/nistpubs /800-145/SP800-145.pdf. [Accessed 5 May 2014].

6. Kuppuswamy, P., and Al-Khalidi, S.Q.Y., 2012. Implementation of Security through Simple Symmetric Key Algorithm based on Modulo 37. *Journal: International Journal of Computers & Technology IJOCT*, 3(2), 335-338.

7. Singla S. and Singh J., 2013. Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm. *Global Journal of Computer Science and Technology Software & Data Engineering,* 13(5), 10-142.

8. Subhasri P., Padmapriya A. (2013) 'Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing', International Journal for Advance Research in Engineering and Technology, Vol. 1, Issue VI.

9. Sunitha, K. and Prashanth, S. K., 2013. Enhancing Privacy in Cloud Service Provider using Cryptographic Algorithm. *IOSR Journal of Computer Engineering,* 12(5), pp.62-64.

10. Suthar, K., Kumar, P., Gupta, H., and Patel H., 2012. Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment. *International Journal of Computer Applications,* 60 (19), 16-19.

11. Workday. (2011). *Are Clouds Less Expensive?* [online] Available at: www.workday.com [Accessed 5 May 2014].