International Journal of Grid Distribution Computing
Vol. 8, No.6, (2015), pp.9-18
http://dx.doi.org/10.14257/ijgdc.2015.8.6.02

An Authenticate Model of Cloud Interaction Using Cryptography

Debabrata Sarddar[1], Nilanjana Das[2] and Joy Halder[3]

[1]*Assistant Professor, Department of Computer Science Engineering, University of Kalyani, Kalyani-741235, India*
[2]*Persuing M. Tech, Department of Computer Science Engineering, University of Kalyani, Kalyani-741235, India*
[3]*Persuing M. Tech, Department of Computer Science Engineering, University of Kalyani, Kalyani-741235, India*
[1]*dsarddar1@gmail.com,* [2]*dasnilanjana286@gmail.com,*
[3]*mailmejoy1991@gmail.com*

Abstract

Cloud Computing is one of the major trends in today's information technology and the most likely research area. Cloud Computing is a model of sharing resources, software, information. The user access the cloud via internet and all the resources are open to all. Thus, cloud security is now a challenging problem for the cloud service providers. Cryptography is a good solution of the cloud security and several research works are published to ensure secure cloud using cryptographic tools. This paper proposes an authentic communication between a customer and cloud service provider using encryption, decryption and message digests.

Keywords: *Cloud service provider (CSP), Authentication Server (AS), Storage Server (SS), Authentication, Encryption, Decryption, Message Digest*

1. Introduction

Cloud computing ('cloud') is a technical term that elaborate the development of many existing Technologies. It mentions to compute on the Internet, rather to desktop. This model defines a convenient and on-demand network access to a pool which is shared depend upon configurable computing resources that can be rapidly scrutinized and released with minimal management efforts [6, 1]. In simple words, Cloud Computing is a total package of a technology and a suitable platform that generally supplied hosting and storage service on the Internet [7]. Every technology leads with a main goal, so here the goal is to provide affordable and scalable on-demand computing infrastructures with good quality of service levels [8]. Here customers don't need to buy the resource from a third party vendor; instead they can use the resource and pay for it as a service thus helping the customer to save time and money and that leads to inexpensive factor of cloud computing. Cloud computing basically is a style of computing in which dynamically scalable and often virtualized resources are provided as a services. With the help of Cloud Computing, IT capacity can be adjusted quickly and easily to accommodate changes in demand [9].Here we come with the next important term of cloud is "as a services". The services that cloud computing hosts provide are broadly divided into three categories:

Software as a Service [SAAS]: It provides a pre-made application, along with any required software, operating system, hardware, and network. The user does not manage or control the underlying cloud infrastructure including network, servers, operating system, storage, even individual application capabilities, with the possible exception of limited user specific application configuration setting [3].

ISSN: 2005-4262 IJGDC

Example: Google Service

Platform as a Service [PAAS]: PAAS [3] is another delivery model, supplies all the resources required to build applications and services completely from the Internet, without having downloaded or install software. The user has control over the deployed applications and possibly, applications and hosting environment configurable, such services include: session management, device management, send box, device integration, testing and instrumentation, content management, knowledge management, UDDI, and XML based registry providing a mechanism to register and locate web service application.

Example: Microsoft Azure

Infrastructure as a Service [IAAS]: IAAS is the next form of service available cloud computing. Where SAAS and PAAS are providing applications to customers, IAAS does not; it simply offers the hardware so that your organization can put whatever they want onto it [3].

Example: Amazon Web Service

Types of Cloud Computing:

Several types of Cloud Computing are as follows [3]:

Private Cloud: Private Cloud refers to cloud computing on private networks. Private clouds are built for the exclusive use of one client, providing full control over data, security and quality of service. Private cloud can be built and managed by a company's own IT organization or by a cloud provider.

Public Cloud: The infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Community Cloud: The infrastructure is shared by several organizations and supports a specific community that has shared concerns.

Hybrid Cloud: A hybrid cloud environment combines multiple public and private cloud models.

Many companies are developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities [3].

Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as Amazon, Google, IBM, Salesforce, Zoho, Rackspace, and Microsoft. It also shares necessary software's and on-demand tools for various IT Industries. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money.

Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises [9]. The world of computing has seen a large number of changes in past few years but just a few of them have had an impact as huge or as industry moving as the arrival of the cloud computing paradigm. By definition Cloud Computing is a style computing in which dynamically scalable and often virtualized resources are provided as a service. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Furthermore, cloud computing employs a model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or

service provider interaction.[6].These technologies are not all new, most of these have been in use in of themselves but they have come to be presented together to hold allow a greater level of flexibility to the user. Educare in their paper "7 things you should know about cloud computing" put it best when they said the term cloud computing refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network [5]. Those resources can include applications and services, as well as the infrastructure on which they operate. By deploying IT infrastructure and services over the network, an organization can purchase these resources on an as-needed basis and avoid the capital costs of software and hardware. With cloud computing, IT capacity can be adjusted quickly and easily to accommodate changes in demand. [1]

2. Related Work

In today's world cloud is very important, now regarding this point it is noted that many companies developed many cloud product and also provide services, but they did not considered the implications of processing, storing and accessing data in a shared and virtualized environment. Now based on this reason we can include & enlighten a new most important topic that is security. Anything that deals with our personal data must have a security checking policy. So by this way it can be assume that cloud also needs security aspect. Security has always been the primary issue for IT executives when it comes to cloud computing and its adoption. However, cloud computing is an aggregation of technology, OS, storage, networking, virtualization each fraught with inherent securely issues.

It also deals with some pitfalls and this is based on the majority of which center around security of the data that is stored in the cloud. Organizations such ISACA and Cloud Security Alliances help to mitigate the security issues in the cloud [6]. First the user information security provides commerce and management and secondly the leakage of information can be caused by technology flows of providers. Cloud Computing is an open environment, so any weakness can cause security risk of the whole system.

There a four important types of security services:

Authenticate: Suppose a sender sends some data to the receiver. Authentication means receiver will get the data coming from the authenticated sender, no other third party cannot claim to be sender [9, 4]. So it is an assurance that the communicating data is same as the data sends by the sender.

Data Confidentiality*:* By the term confidential it can be said that the data is hidden from any third party. Only the sender and receiver are able to access the data, not anyone else [9][4].

Data Integrity: The assurance that data received are exactly as sent by an authorized entity (*i.e.*, contain no modification, insertion, deletion, or replay) [8, 2].

Non Repudiation It provides protection against denial of services by one of the entities involved in a communication of having participated in all or part of the communication [9].

Cryptography is the practice and study of hiding information. Cryptography referred almost exclusively to encryption, which is the process of converting the plaintext into unintelligible gibberish *i.e.*, cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext.

Symmetric Key Cryptography: Symmetric encryption is one type of cryptosystem in which one key is used for both encryption and decryption [9, 2]. For example DES Cryptography.

Asymetrix Key Cryptography: Here two different key is used, one key is used for encryption (public key) and other key is used for decryption (private key) [9].

Assume, each entity possess a set of (private key, public key) pair. One popular algorithm to calculate this type of key pair is RSA algorithm [9] describes below:

Select two large prime number p and q ($p \neq q$)
Calculate n = p * q
Calculate $\emptyset(n) = (p - 1) * (q - 1)$
Select integer e (encryption key) such as
gcd ($\emptyset(n)$, e) = 1; $1 < e < \emptyset(n)$
Calculated d (decryption key) such as
$d \equiv e^{-1} \pmod{\emptyset(n)}$
Encryption by B
Cipher text: $C = M^e \bmod n$
Decryption by Alice with Alice's Public Key
Plaintext: $M = C^d \bmod n$

The following table is derived by one of the authors of RSA come in scenario in 1978. They hold an operation in the Schroeppel factoring algorithm takes one microsecond to compute, and present the following data for various lengths of n:

Table 1.

DIGITS	NUMBER OF OPERATIONS	TIME
50	1.4×10^{10}	3.9 hours
70	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^{9} years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

Message Digest: Message digest is a method (hashing) to map a variable length data block into a fixed length non readable format. A good hash function never left any clue of the original text in calculated hash value. Popular algorithms for calculating message digest are MD5 (128 bit), SHA 1 (160 bit) *etc* [9].

This paper proposes an authentic and secure connection between a customer and cloud service provider using encryption, decryption and message digest.

3. Proposed Work

According to proposed model, Cloud Service Provider (CSP) is a trusted authority and is responsible for all decisions and activities. Authentication Server (AS) and Storage Server (SS) are two organizations under the supervision of CSP and their functions and activities are controlled by CSP.

First of all the CSP, AS and SS maintain a model which is solely dependent on a set of Public Key and Private Key. Now the second constraint is Public key of CSP is open to all, and only CSP knows the Public key of AS and SS. So no other third party can use the Public Key, only CSP is able to use the Public Key of AS & SS, but if any third party wants to communicate with AS or SS, then she has to communicate with CSP first. If CSP grants the third party to communicate with the AS or SS, then she can do so. In this model the third party never knows the Public Key of AS or SS but she can securely communicate with them.

Here, three layer of security checking is performed to ensure authentication. In the 1st phase, customer sends a request to CSP then the connection will be established between customer/third party and CSP, in the 2nd phase AS verifies the previous connection and authenticates the customer. In the last phase, customer receives information about Storage Server (SS) and communicates with SS.

Working Model

To ease of understand, we use some notation to describe our model. We discuss each phase elaborately and describe the notations when they are needed.

1st phase:

Suppose, customer sends a package to CSP including the following information and objects:

User's login information

User's public key

User's current location

User's id which is encrypted by CSP's public key, where user's id may be voter card number or SSN number that uniquely identify the user. User's id will be denoted as user-id.

Time-Stamp (TS)

User always remembers his/ her Time-Stamp (TS) and waits for CSP's response.When CSP receives the package, CSP first decrypt user-id using its private key and searches its database against the user-id to check whether the customer is fake or not. If the customer is verified positively, CSP does a set of action as follows.

CSP Enlist the Customer's Name.

CSP calculates message digest (M) of user-id using some standard message digest algorithm (MD5 or SHA1).

M= message-digest (user-id)

Now, user stores M against username, note if somehow an attacker is able to access the Database of CSP, he will find the message digest of user-id in spite of original user-id.

CSP creates two session keys K1 and K2. Encrypt K1 by AS's public key, encrypt K2 by SS's public key. We already discussed that only CSP knows the public key of AS and SS.

Let, A = $E_{Pub-AS}(K1)$

B = $E_{Pub-SS}(K2)$

CSP calculates two time intervals T1 and T2, in which the customer communicate with AS and SS, where (T2>T1).

Let, P1= address of AS,

P2= address of SS,

CSP now sends some information so that customer can securely communicate with AS and SS.

Let, X= [A+ (TS+T1) +P1]

Y= [B+ (TS+T2)]

CSP encrypts X and Y using customer's public key and sends to customer.

CSP encrypts [P2+M + (TS+T1) + (TS+T2) + user's public key] using AS's Public key and sends to AS.

2nd Phase:

After receiving the packet information from CSP the customer decrypts all the packet and retrieve all the information. Then customer finds the address of AS (P1) and the time limit to create connection with the AS and SS (T1, T2) but cannot open A and B, as she is

unknown about the public key of AS & SS. Customer now calculates the message digest of his user-id (M1) and after that she creates a package including the following data,
Z= A+M1 + TS' (current time-stamp)

And sends it to AS, as she now knows the address of AS.

AS already receives the packet send by CSP and retrieves all the data by decrypting its private key. After receiving the packet, AS does the following action:

AS checks if TS+T1<TS' or not that is the time limit is over or not, if so, AS replies customer as time out message and ask her to log in again.

If customer packet reaches within time interval, AS checks A which is encrypted by its own public key, which is known to CSP only, but not to the customer. So it is the same customer who communicates with CSP.

There may be a number of customers who creates communication with CSP, so AS further matches M and M1, two messages digests –one received from CSP and another from customer.

When all the checking are done positively, AS now creates a session key K3, encrypt it with SS's public key, and creates a data packet:
W= [$E_{Pub-SS}(K3) + P2$]

AS sends W to customer.

AS sends encrypted M along with (TS+T2) using SS's public key and send it to SS.When the customer again receive the data set from AS, the customer retrieves all the data using its private key. Again the customer finds the address of the storage server, but cannot open K3, the customer, again creates another packet containing encrypted K3,B, M1 (message digest of user-id) and current time stamp (TS") are send to SS.

SS receives the packet from customer, finds encrypted K3 and B by its public key; and does the following:

S checks if TS">TS+T2, that is if the time limit is expire or not. If yes, SS asks the user to log in again.

B is encrypted by CSP; so it is the same customer who has communicated with CSP and now communicating with SS.

K3 is encrypted by AS, so again the same customer who is communicated with both AS and SS.

What will happen if some attacker is able to hack both B and encrypted K3? This scheme is still Secure as the attacker cannot have the user-id of the original customer, so he cannot calculate the M1. Thus, SS now matches M' with M receive from AS.

Finally, all the authentication checking is performed and SS informs CSP that the customer whose message digest of user-id is M, authenticated securely. CSP then informs the customer that she successfully logged in and asks the customer to follow SLA instructions and one time password to communicate with SS.

4. Performance

In this Section, we present use of every component used in this model and also describe some odd situations and how they are overcome using this model.

The customer obtains the CSP's public key.

CSP is a well-known authority, so it is obvious that everybody who wants cloud services from CSP must know the public key of CSP, as it is public for everyone.

The customer sends his public key to CSP.

There are a number of users who needs cloud service. But CSP is unaware about them until they send their log in information with her public key.

The customer sends her user_id.

How the CSP knows this it is the original customer who is claimed, so customer sends her id, encrypted by CSP's public key. So, only CSP now able to open it, then check its database and authenticate the customer.

CSP stores message digest of user_id.

User_id is the only key to authenticate a unique customer so instead of storing the user_id, CSP stores the message digest (M) of user_id in its database. If anyone is able to find, he will get the M, not the original user-id.

How the customer is authenticated between AS and CSP?

CSP creates K1 and encrypted using AS's public key (A). So, only AS can open it. Customer sends A to AS, and A can be created only by CSP, hence it is the same customer.

AS match's two message digest of user_id, M and M1, one received from CSP and another from customer.

Customer gets the address of AS (P1) from CSP.

How the customer is authenticated between AS and SS?

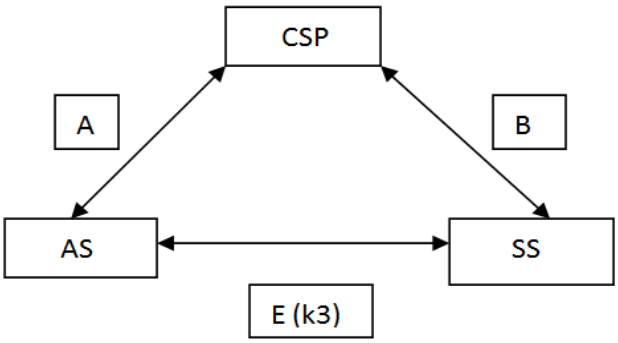
AS creates K3 and encrypts using SS's public key. SS's public key is known to AS, but not to the customer. Thus when customer sends the encrypted K3 to SS, authentication checking is done.

SS matches two message digest of user_id, M, M1, one received from AS and another from customer.

Customer gets the address of SS (P2) from AS.

How the authentication is verified between CSP & SS?

CSP creates K2 and encrypts it using SS's public key (B). SS receives it from customer.



Function of time-interval T1 and T2:

This scheme use two times interval T1 and T2 to add a constraint to user to contact with AS & SS. Time intervals T1 and T2 are created by CSP. The time intervals are so calculated that it is enough to create a communication but not to decrypt A or B or encrypted K3. For security, Public keys of AS and SS are not open to customer, but she receive A, B and E (K3). To prevent the decryption of A, B and E (k3) to obtain the public key of AS and SS, CSP limits the time to T1, T2 and beyond this time interval, no connection requests are accepted.

5. Conclusion and Future Work

So far in this paper, we introduce a model to ensure authentication when a user creates a connection with CSP. Several works and journals are published regarding to this approach. Cryptography is now the one of the main way to provide cloud security, so we will try to use more complex encryption process like AES, El Gamal encryption technique, elliptic curve encryption to provide cloud security. In this above approach, we assume that the customer wishes to connect with single storage server (SS), but in near future we will work on the conditions when the customer migrates from one storage server to another server or CSP provides the customer Elastic IP, a set of address of addresses of several storage servers (SS). We also try to add data integrity and confidentiality in the described future works.

Reference

[1] B. Chandrasekhar, M. Derick, and K. A. Sumithra Devi, "A Flexible Interface for Security Issues in Cloud Computing".
[2] D. Akansha, K. Janda Harneet, B. Sayalee, "Security on Cloud Using Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 3, (**2015)** March ISSN: 2277 128X.
[3] F, Borko, E. Armando, M. Dan C, "Handbook of Cloud Computing, Springer Cloud Computing: Theory and Practice".
[4] K. Jashanpreet Pal, K. Rajbhupinder, "Security Issues and Use of Cryptography in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X vol. 4, issue 7, **(2014)** July.
[5] M. Dr. Prerna & S. Abhishek. "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13 issue 15 Version 1.0 Year **(2013)** Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
[6] M. Prince Jain Polytechnic College Faridkot, Punjab-151203, India prince12.jain@gmail.com, "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research ISSN (Online): pp. 2229-6166.
[7] E. Mills, "Cloud computing security forecast: clear skies," *CNET News*, **(2009)**.
[8] S. Joachim, "Cloud Services", 4th IEEE International Conference on DEST, Germany, **(2010)**.
[9] S. William, "Cryptography and Network Security Principles and Practice Fifth Edition" Pearson, BBS, **(2011)**.

Authors

Debabrata Sarddar is an Assistant Professor at the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India. He completed his PhD from Jadavpur University. He did his M. Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.E in Computer Science & Engineering from NIT, Durgapur in 2001. He has published more than 75 research papers in different journals and conferences. His research interests include Wireless and Mobile Systems and WSN, and Cloud computing.

Nilanjana Das, B.Tech pass out from College of Engineering and Management, Kolaghat, Pursuing M.Tech, Department of Computer Science and Engineering, University of Kalyani, Kalyani-741235, India.

Joy Halder, B.Tech pass out from Academy Of Technology, Pursuing M.Tech, Department of Computer Science and Engineering, University of Kalyani, Kalyani-741235, India.

