Security-SLA and Signature Scheme for Cloud Network

Abhishek Pandey
Research Scholar
Dr.C.V.Raman University
Kota, Bialspur C.G.-India

R. M. Tugnayat, Ph. D
Principal
SSA College of Engineering
Wardha-M.S.-India

Anil Tiwari, Ph. D
Principal
Disha College
Raipur C.G.-India

ABSTRACT

Cloud Computing is used for management of resources applications and information as services over the cloud. The resources used in Cloud are usually distributed as services. Cloud resources are majorly delivered to the customers in terms of services and the security here is implemented through the infrastructure security metrics via a Service Level Agreement (SLA). SLA is a legal framework between the provider and the user. In this paper we provide a comprehensive model that concentrates more on security issues. Here we try to generate security SLA which is different from traditional security as it deals with the service levels related to cloud security as in our work and see how it deals with the metrics related to security. We will also verify the security metrics through the Security SLA (SSLA).In this paper a signature based scheme based on Canonical Form Prime Factorization is also proposed.

General Terms

Security Metrics, Service Level Agreement, Cloud Security Framework, Signature Based Security Scheme.

Keywords

Cloud Computing, Service Level Agreement (SLA), Security Metrics, Cloud Security.

1. INTRODUCTION

Cloud computing is considered to be a latest method of distributing computer resources .The resources used in Cloud Computing are the resources that are usually distributed as services.

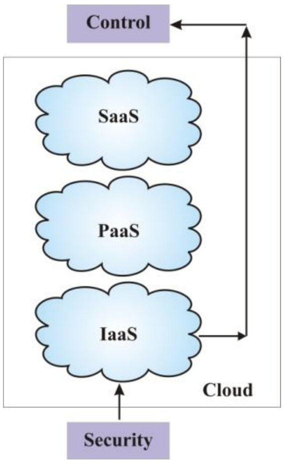

Fig1: Cloud control and security

Fig1 shows the user control over the services and how it is related to security. The cloud computing service architecture falls under three categories of services and there exist four deployment models. The services posses its own unique fundamental characteristics that distinguish them from the traditional computing environment. Cloud computing uses internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access.

The technology behind cloud allows much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is an innovative technology that facilitates the networked nodes to share the pooled resources on demand in pay per use model. Resources could be a simple software application, a platform needed for project development or the infrastructure itself using Internet as the backbone. Service Level Agreements (SLAs) in the Cloud serves as both the blueprint and warranty for cloud computing.

2. SECURITY METRICS(SM) FOR CLOUD

The cloud is entirely un-trusted. It may return arbitrary data for any request from the owner or any user. Further, the cloud may not follow the access control lists created by the owner and send values to a user not on the corresponding access control list. A user is trusted with the data he/she is given access to. However, he/she may attempt to subvert limits on his permission to access data, possibly in collusion with the cloud. An owner is trusted with accessing the data because it belongs to him. However, the users and the owner may attempt to falsely accuse the cloud of violating one of our security properties. In this paper we will identify information security attributes relevant in cloud computing.

Security metrics are quantitative measurements to assess security operations in organization environment [1]. They aid the organization to make decisions about various aspects of security which include security architectures and controls to the effectiveness and efficiency of security operations [2].The Security Metric should be measurable and quantifiable and which is often a main concern when it comes to security of cloud network. The metrics is responsible for security policy formalization and evaluation also [3.]The security metrics should be goal specific [4].

3. PROPOSED FRAMEWORK

3.1 Security Service Level Agreement (SSLA) in Cloud

Main focus here is aimed at creating an open-ended, flexible framework which will be able to extend through the integration of new security metrics for specific purposes.

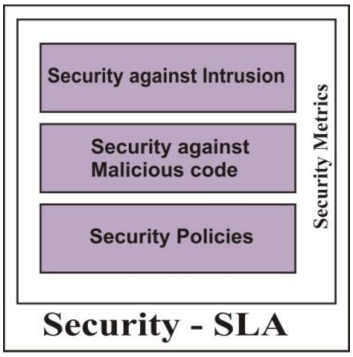

Fig2: Security Service Level Agreement

Security levels in cloud are treated in separate SLA i:e SSLA.The proposed framework The proposed framework is *objective and quantitative* based structure to provide a secured environment and also act as a decision maker in selecting out of the various offerings by the cloud. The figure shows how the metrics helps in selecting a particular services offered by the cloud through the metric definition.

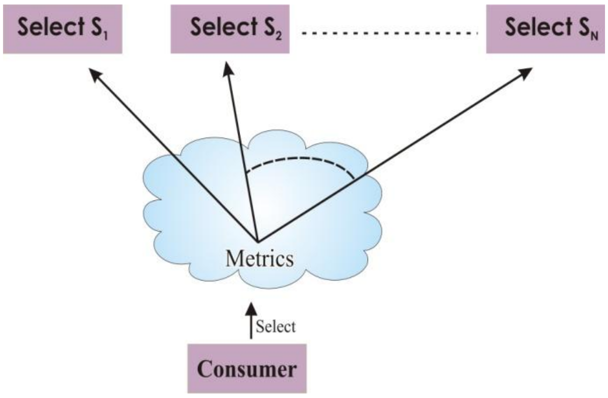

Fig3: Selection of cloud services based on metrics

Here the metrics helps to make a decision in selecting the Service from S_1 to S_N based on the definition. Then the decision is taken on selecting the service from the cloud services being offered. SSLA helps to monitor the services being utilized by the customer. In above case it selects S_1.The table below shows an example metrics as proposed by [5]

Table1: Metrics and their functionality

Metric	Functionality
Password Management PSWD-MGMT	Describes how many times and how often the password can be modified.
Backup-BKP	Policies for the backup along with the time.

The SSLA is concerned to the quality of service being delivered. As defined in table 1 the Backup metric is responsible for policies for taking up the backup. The key factor here will be the location for this backup along with defining the time limit for the backup to take place. The format for backup of the data is governed by the client along with the time duration for this backup to take place. The table shows the metrics for the backup. Once the agreement is set between the cloud customer and the provider, the other important issue will be monitoring the the SSLA through an interface.

Table 2: Metrics Description

Metric	Description
Frequency	Half-Hourly
Location	Dedicated Server
Format	As decided by the client.

The primary entities here are the cloud service users, the various applications being utilized by the clients and the team of IT experts monitoring the resources, platform and services being used. The monitoring focuses on the the actions of these entities. Here a check for the SLA is met or not once the SSLA is configured. The integrity and confidentiality is also checked here depending upon the parameters as described in SSLA.The proposed framework tries to meet the various objects of cloud computing. The basic object in cloud can be depicted as [6]

Table 3: Cloud Objects

Sr.No	Object
1	Configuration Management
2	Change Management
3	Problems and Incident Management
4	Risk Management
5	Compliance Issues
6	Operation Management
7	Performance and Capacity Management
8	Continuity of IT services
9	IT security Management
10	Software Management

For each object a SSLA based Metric is defined and parameters are set to achieve an assurance of the target being met. Cloud security metrics are similar to other measures of security effectiveness, and also for the general business measures. The Cloud metrics are well defined and collective in nature and also they support the questions related to specific goal or the target providing a higher level of abstraction.

3.2 Security in Cloud

The issues related to security in cloud can be classified as [7]data issues, privacy issues and security issues. Further it can be classified as so as to answer: Privacy, Integrity and Verifiability [8]. These parameters can be summarized keeping in view the basic architecture of cloud as shown in fig. Security in cloud can be managed in 2 ways:

a) Deriving method of authentication and authorization.

b) By encrypting the data in the cloud.

The main task is to find what are the information security attributes are relevant in cloud computing. This research question is formulated in order to identify information security attributes relevant in cloud computing with the cryptographic techniques and SLA’s thus making it a hybrid model. The answers to this question also assist us to identify information security metrics in cloud computing. The proposed enhanced security framework is an efficient security framework that incorporates the various security preserving cryptographic techniques. Here a multiple stage authentication process which will be usually adopted for user authentication at the server end for data access in a simple two or three tired client server architecture.

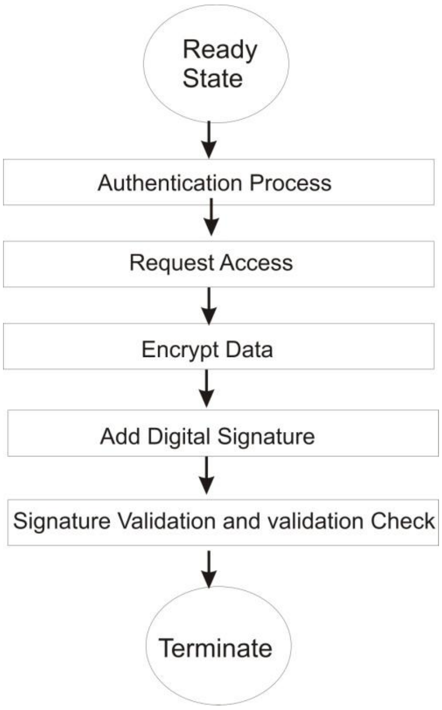

Fig4: Security process

3.3 Signature Scheme for Cloud

In the proposed scenario we use a signature scheme based on Canonical Form Prime Factorization[9]. If (a) is a positive integer greater than 1, then (a) has a prime factor. But if (a) writes as : $a = p_1^{\alpha_1}\, p_1^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$ Where $p_1 < p_2 < \cdots < p_n$ and where P's are positive prime and $\propto_1, \propto_2, \ldots. \propto_n$ are positive integer ≥1. So this refers as Canonical Form of Prime Factorization. The algorithm of the proposed Signature scheme can be depicted as:

1. Let message = m.
2. The Prime Nos. : p_1,p_2,….,p_n
3. Positive integers : $\propto_1, \propto_2, \ldots. \propto_n$
4. $a = p_1^{\alpha_1}\, p_1^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$ and Euler's Totient function[10] is : $\emptyset(n) = \emptyset(P_1)\emptyset(P_2)\ldots\emptyset(P_n)$
5. Selection of e_1, e_2 by:

   $1 < e_1 < \emptyset(a)$ and $\gcd(e_1, \emptyset(a)) = 1$

   $1 < e_2 < \emptyset(a)$ and $\gcd(e_2, \emptyset(a)) = 1$
6. Determine d by:

   $d = e_1 e_2 mod\emptyset(a)$
7. $m' = m_{e_1}^{e_2} mod\emptyset(a)$
8. $s' = (m')^d mod\emptyset(a)$
9. $s = s'.e_1^{-e_2 d} mod\emptyset(a)$

The same can be determined through an Example

1. m
2. $P_1 = 3, P_2 = 5.$
3. $\propto_1 = 2, \propto_2 = 4.$
4. $a = (3)^2\ (5)^5 = 5625$

   $\emptyset(a) = \emptyset(3)\emptyset(5) = (3-1)(5-1) = (2)(4) = 8 = \emptyset(5625)$
5. e_1: $1 < 3 < 8$ *and* $\gcd(3,8) = 1$ and

   e_2: $1 < 5 < 8$ *and* $\gcd(5,8) = 1$
6. $d = (3)(5)mod(5625) = 15mod(5625)$
7. $m' = m(3)^5 = mod\emptyset(5625)$
8. $s' = (m')^{15} = 15mod\emptyset(5625)$
9. $s = s'(3)^{-5X15}\ mod(5625)$

   $= (m')^{15}\ 3^{-75}$ mod(5625)

   $= (m.3)^{15}\ 3^{-75}\ mod(5625)$

   $= m.3^{75}\ 3^{-75}\ mod(5625)$

   = m

The Secret keys are never stored in plain form and the Symmetric keys for a specific resource exist in memory only, and are decrypted for use only when the actual data is needed, then they are discarded. A secure information transmission protocol is developed to realize a message transfer between the two parties through which the client and the server could determine the similarity of data without revealing their secured data and compromising the security. Here, the client reconstructs the server side data and determines that the client data is same giving an edge in the secured transmission in cloud environment. When the user is accessing the services (SaaS Application) a token is sent to SaaS which validates the token which in turn allows the user to access the desired services. In this process the SaaS upon validating the token uses its contents. Here the application uses the information contained in the token to decide the limit of accessibility to the user as shown in the figure.

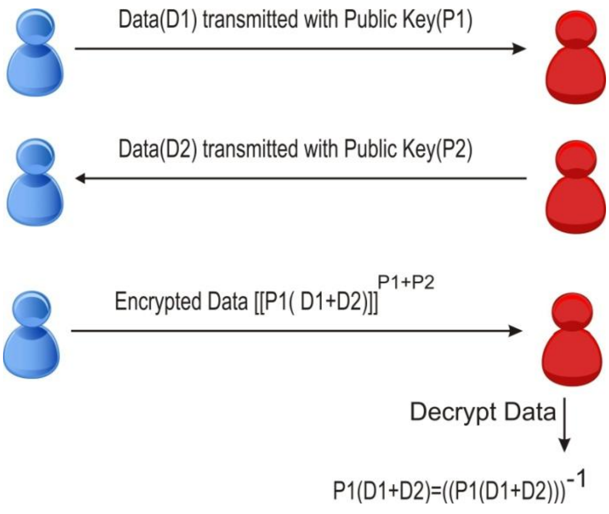
Data(D1) transmitted with Public Key(P1)
Data(D2) transmitted with Public Key(P2)
Encrypted Data [[P1(D1+D2)]]^P1+P2
Decrypt Data
P1(D1+D2)=((P1(D1+D2))^-1

Fig5: Secured Transmission in cloud

4. CONCULSION

In this paper, model for the security SLA which is different from traditional security as it deals with the service levels related to cloud security as in our work and we identified the information security attributes relevant in cloud computing. We also saw how the integrity and confidentiality is also checked here depending upon the parameters as described in SSLA The main objective was to propose an approach for the encryption in the verification process in the form of signature scheme based on canonical Form of Prime Factorization.

5. REFERENCES

[1] J Andrew, Security Metrics Replacing Fear, Uncertainty and Doubt: Addison Wesley, 2007.

[2] W. Jansen, "Directions in Security Metrics Research,NISTIR 7564," NIST, 2009.

[3] Jesus Luna, Hamza Ghani, Daniel Germanus and Neeraj Suri , A security framework for the cloud In Proc. of the International Conference on Security and Cryptography (SECRYPT), 2011

[4] Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas, 2012. “Cloud Computing Synopsis and Recommendations,” *NIST Special Publication 800-146*, May–http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

[5] “Security Perspective in Security Management for Cloud Computing” A.S.Chaves, C.B.Westphall and F.R.Lamin, 2010 Sixth International Conference on Networking and Services, INE5619-06238.

[6] COBIT is an IT governance framework and supporting toolset - see http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[7] Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/../ProblemsFacedbyCloudComputing.pdf.

[8] “Cryptography Challenges for Computational Privacy in Public Clouds” Sashank Dara, in the proceedings of IEEE 2013 CCEM Conference.

[9] Phani Bhushan Bhattacharya, Surender Kumar Jain, S. R. Nagpaul, Basic abstract algebra, Theorem 5.4, p.423.

[10] Sandifer, Charles (2007), The early mathematics of Leonhard Euler, MAA, ISBN 0-88385-559-3.