Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Colouring by cloud Watermarking using RSA for Periodic Authentication

I. Sudha, P. Jamuna
Assistant Professor, Department of CSE
Achariya College of Engineering Technology Puducherry, India

Abstract— Cloud Computing has been envisioned as the next generation style of computing for cost effective IT services .Cloud Computing face the overwhelming challenges to ensure the proper physical, logical and personnel security controls, especially while moving huge volumes of data and softwares to the large data centers. To protect clouds, CSP (Cloud Service Providers) must first secure virtualized data center resources, maintain user privacy, and preserve data integrity With Virtualization technology, cloud computing offers diverse services (such as virtual computing, virtual storage, virtual bandwidth, etc.) for the public by means of multi-tenancy mode. Cloud security hinges on how to establish trust between these service providers and data owners in the virtual storage environment. We provide a data coloring technique based on cloud watermarking can significantly result to make the system robust as well as secure user's data. However these techniques strengthen the authentication mechanism for accessing the data in the cloud service provider, there is a possible way of misusing the data from intruders .To ensure the security of data , we propose a method of providing security by using RSA algorithm for the periodic authentication to ensure whether the legitimate users are accessing the data.

Keywords— Cloud computing, cloud security, cloud watermarking, data coloring, secure RSA Algorithm

I. INTRODUCTION

Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Cloud computing is an emerging business model that delivers computing services over the internet in an elastic self-serviced, self-managed cost effective manner with guaranteed quality-of-service (qos).

The four cloud deployment models are described as below in Fig.1:

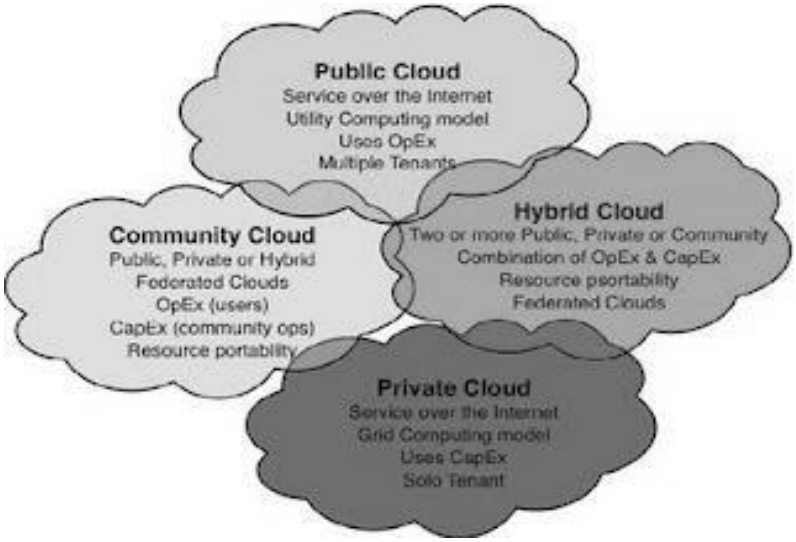

Fig. 1 Deployment models of Cloud Computing

- **Private cloud:** A Private cloud can be deployed on existing on-premises computing infrastructure using open-source cloud software or third-party commercial offerings to meet the needs of an organization.
- **Public cloud**: A public cloud provides computing services that are publicly accessible through standard self-service APIs over the Internet.

© 2013, IJARCSSE All Rights Reserved

- **Hybrid cloud:** A Hybrid cloud is a mixed deployment model, employing both private and public infrastructures. A hybrid cloud is mostly used for offloading processes and/or data to a public cloud while maintaining the desired degree of control inside a private cloud.
- **Community cloud:** A community cloud is a collaborative effort in which infrastructure is shared among several organizations and supports a specific community with common concerns. It may be managed by the organizations or a third party and may exist on premise or off premise

II. SECURITY ISSUES IN CLOUD COMPUTING

Time, cost, innovation leads to the success of cloud computing but still there are certain security concerns that need to be addressed while moving critical applications and sensitive data to public and shared cloud environments. Major security issues faced by cloud providers and by their customers are discussed below:

1. ***Location of Data*:** Various organizations located in different places have different needs and controls placed on access. Because the data is in the cloud, one may not realize that the data must reside in a physical location. The cloud provider should provide the level of security required for different customers and their needs.

2. ***Access to data*:** Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone using the cloud need to look at who is managing their data and what types of controls are applied to these individuals.

3. ***Data classification**:* Is the data classified? How is your data separated from other users? What is the type of Encryption mechanism?

4. ***Service level agreement (SLA) terms:*** Organizations need to ensure the security and integrity of their data, even when it is held by service providing the cloud. They also need to prove conformity with security standards regardless of the locations of their data and applications. This could be achieved by Service Level Agreements (SLA), Loss of service, Audit, and service conformity

5. ***Security breach:*** If a security incident occurs, what support received from the cloud provider?

6. ***Privileged access*:** This is the question about who has the privilege to access the data. Who is responsible for hiring & management of the administrators, which handles the information?.

7. ***Authentication and authorization**:* Every organization has its own way to manage authentication and authorization. Every organization must determine if its current authentication system could also work in a secure and reliable way for users in a cloud environment. Apart from that what is the best way to authenticate cloud services but also be insured.

Security concerns based on delivery and deployment models are data integrity, data locality, data confidentiality, and data access. Some more security related concerns are Sign on process, Authentication & authorization, network security, identity management and especially multi-factor authentication which considers multiple factors together for authenticating a user.

A. *CIA triad:*

A security framework for an information system has three goals namely confidentiality , integrity and availability.

B. *AAA:*

The security framework for an information system should provide authentication and authorization capabilities.

C. *Defense-in-Depth:*

It is a risk management strategy which provides multiple layers of defense against attacks.

D. *Multi-factor authentication:*

- **First factor:** What does a user know? For example, a password for a log in session will be what a user is required to know.
- **Second factor:** What does a user has? For example, a user needs to provide a secret key , generated by a physical device (token), which is under the user's possession.
- **Third factor:** Who is the user? For example, a biometric signature of a user can be considered as an example of who is a user id.

III. THE CLOUD MODEL

This model is a transform of quantitative and qualitative data. Suppose U is a universal set of numbers, C is a qualitative concept related to the universal set U. Any variable x that belongs to universal set U i.e. $x \epsilon U$ randomly realized the concept C with the certainty degree of x for C.

A random value lies between 0 and 1 [9].

$$\mu: U \rightarrow [0,1], \quad for\ all\ x \epsilon U \quad x \rightarrow \mu(x)$$

© 2013, IJARCSSE All Rights Reserved

The distribution of x on U is defined as a cloud and every x is defined as a cloud drop. In this model, the property of cloud drops is represented by Ex i.e. expected value, En i.e. entropy and He i.e. hyper entropy where the expected value is a mathematical representation of cloud drop. We can also say that a cloud drop is located at some point Ex is most recognizable value of qualitative concept. En connects the concepts of both randomness and fuzziness by granularly measuring the qualitative concept.

IV. DATA COLOURING TECHNIQUE

The difference between traditional watermarking and cloud watermarking is that in cloud watermarking it just not only embeds the user's copyright information but it also colors all of its data. Each of the users is specified by a color that helps to protect the copyright and also avoids the manipulation of original data.

The following Fig.2 shows the forward and backward color-generation process. The cloud drops are added into the input photo (left) and remove color to restore the original photo (right).The process uses three data characteristics to generate the color: the expected value (*Ex*) depends on the data content known only to the data owner. Whereas *entropy* (*En*) and *hyperentropy*(*He*) add randomness or uncertainty, which are independent of the data content and these three functions generate a collection of cloud drops to form a unique color that the providers or other cloud users can't detect. This technique can also be applied to protect documents, images, videos, software, and relational databases in the cloud. The Fig.2 shows the details involved in the color-matching process, which aims to associate a colored data object with its own, whose user identification is also colored with the same *Ex*, *En*, and *He* identification characteristics. The color-matching process assures that the colors applied for user identification match the data colors. This process initiates authentication and authorization.

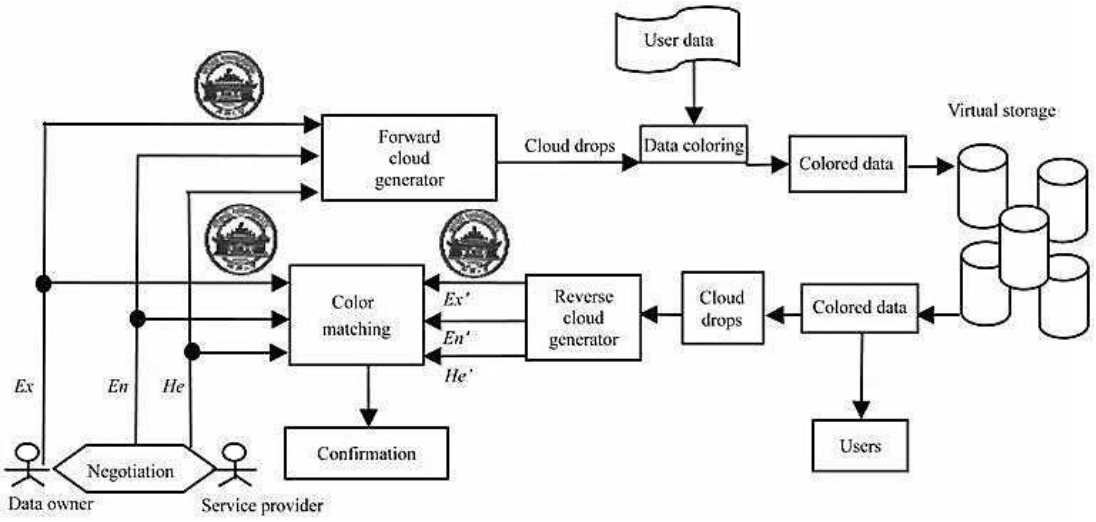

Fig. 2 Data coloring with cloud watermarking

V. DATA PROTECTION IN CLOUD

Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. The best possible solution to deal with Security issues is Data Encryption. Various algorithms exist to encrypt the data in Cloud Computing such as DES, 3DES, blowfish, AES, RSA, etc. Cloud storage concern the user does not have control over data until the user has been gaining access. To provide control over data in the cloud data-centric security is needed. Before accessing the data it should satisfy the policy rules already defined. So cloud should enforce this scheme by using cryptographic approaches.

VI. BASE METHODOLOGY

Each Cloud user is provided with a value called expected value which is known only to the user and the negotiated values with the CSPs are Entropy which is unique for all users in the particular group sharing the data in the cloud and Hyper-entropy is the value which is common to all the group users of the data.To provide the continuous authentication within the group, an automated validation using the tiny bit of data can be made at regular intervals of time.The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.

The basic steps of RSA algorithm are represented as in the Fig.3

- **Key generation**
- **Encryption and**
- **Decryption**

© 2013, IJARCSSE All Rights Reserved

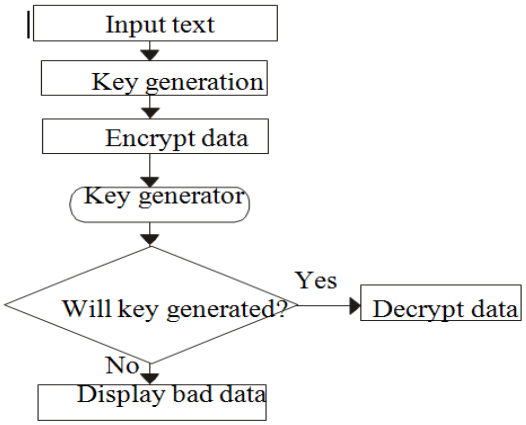

Fig. 3 Execution flow of the entire process

The algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key

Step 1: Select two prime numbers.
Step 2: Calculate n = p*q.
Step 3: Calculate f(n) = (p-1)(q-1)
Step 4: Select e such that e is relatively prime to f(n) and less than f(n).
Step 5: Determine d such that de congruent modulo 1 (mod f(n)) and d<f(n).
Step 6: Public key = {e, n}, Private key = {d, n}
Step 7: Cipher text c = message ^{e} mod n
Step 8: Plain text p = ciphertext ^{d} mod n.

VII. CONCLUSIONS

Cloud computing is revolutionizing the way business is carried out in various industries (Government, Healthcare, Software etc.), use of information technology resources and services, but the revolution always comes with new problems. One of the major problems associated with Cloud computing is Security. The proposed system has many advantages over the existing system. The proposed system has the most secure authentication mechanism in accessing the data because, a periodic authentication is made to ensure whether the legitimate users are accessing the data in the cloud.By using RSA algorithm, the key is generated to ensure whether the legitimate users are accessing the data in the cloud and continuous monitoring will be taken by providing periodic authentication. This paper also discusses the advantages, features, services on the cloud and the different deployment models .In the future, security algorithm will be implemented producing results to provide periodic authentication for cloud users .

REFERENCES

[1] Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li, Gui-Sheng "A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking" ,IJAC Aug 2011.
[2] Kai Hwang "Trusted Cloud Computing with Secure Resources and Data Coloring" Volume: 14, Issue: 5, IEEE Sept 2010.
[3] William Stallings, ―Cryptography and Network Security Principles and Practices, Prentice Hall, New Delhi.
[4] zhiguo du, dahui hu, "image watermarking technology based on cloud model", asia pacific youth conference on communication technology, pp.25.27,2010.
[5] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).
[6] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing (DASC 09), IEEE CS Press, 2009.
[7] Cong, W.,W.Qian and R. Kui, 2009. Ensuring Data Security in Cloud Computing. IEEE.
[8] wayne jansen, "guidelines on security & privacy in public cloud computing", special publication 800-144, national institute of standards & technology.
[9] G. Lo-Varco, W. Puech, W. Dumas. Content based watermarking for securing color images. Journal of Imaging Science and Technology, vol. 49, no. 5, pp. 464-473, 2005.
[10] joshi akshay "enhancing security in cloud computing", information & knowledge management, vol.1,no.1, pp.40-43, 2011.
[11] Cyril bazin, jean marie, "a novel framework for watermarking", springer-verlag berlin Heidelberg,pp.201 217, 2008

© 2013, IJARCSSE All Rights Reserved