IJCRR
Vol 04 issue 21
Section: Technology
Category: Research
Received on: 29/08/12
Revised on: 12/09/12
Accepted on: 20/09/12

AN AUTHENTICATION IN CLOUD THROUGH DATA COLORING USING PROGRESSIVE APPROACH

S. Sandosh, S. Uthayashangar

Manakula Vinayagar Institute of Technology, Puducherry, India

E-mail of Corresponding Author: s_sandosh@yahoo.co.in

ABSTRACT

Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, CSP (Cloud Service Providers) must first secure virtualized data-center resources, maintain user privacy, and preserve data integrity. Using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners is becoming mandatory. Data coloring and software watermarking techniques protect shared data objects and ensures the security level in the cloud. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and strengthen the security for accessing confidential data in both public and private clouds.

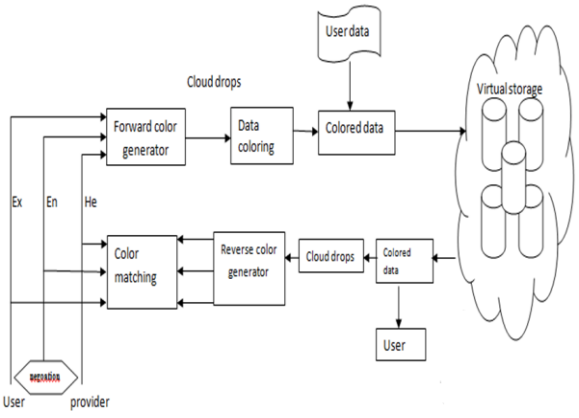
However the problem is, once the onetime authentication is done with Cloud Service Provider (CSPs), there is no guarantee that only the legitimate user is accessing the confidential data and maintaining privacy till the user quits the secured cloud. Hence to provide the continuous authentication the proposal has been designed.

Keyterms :- Cloud computing, Data coloring, Progressive Approach, Secure Hash Algorithm-1.

INTRODUCTION

Cloud computing supports the business model that supports pay-for-use, E- business and many IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centers. Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. However, there presence a lack of trust between cloud users and Cloud Service Providers has slowed down the universal acceptance of clouds as outsourced computing services. To promote the cloud more secure, trustworthy, and dependable, the design of the new cloud ecosystem has become mandatory.

In reality, trust is a social problem, not a purely a technical issue. To increase the adoption of Web and cloud services, *cloud service providers* (CSPs) must first establish trust and security to look up the worries of a large number of users. A healthy cloud ecosystem should be free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations.



Data integrity issues in the cloud differ from those in traditional database systems. Cloud users are in worry about whether data-center owners will abuse the system by randomly using private datasets or releasing sensitive data to a third party without authorization. Cloud security hinges on how to establish trust between the Cloud Service Providers (CSPs) and data owners. To address these issues, a reputation-based trust-management scheme augmented with data coloring and software watermarking is prepared and proposed.

EXISTING SYSTEM

Data coloring: *The* architecture uses data coloring at the software file or data object level. This lets us segregate user access and insulate sensitive information from Cloud Service Provider CSP's access.

Watermarking

The cloud computing's use of shared files and datasets, an user could compromise privacy, security, and copyright in a cloud computing environment. The user needs to work in a trusted software environment that provides useful tools for building cloud applications over protected datasets. In older days, watermarking was mainly used for digital copyright management. Later some experts have suggested using watermarking to protect software modules. The trust model Deyi Li and his colleagues propose offers a second-order fuzzy membership function for protecting data owners. This model is extended here to add unique data colors to protect large datasets in the cloud.

The above Figure shows the forward and backward color-generation processes. The cloud drops (data colors) is added into the input photo (left) and remove color to restore the original photo (right). The coloring 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 Collectively, these three functions generate a collection of cloud drops to form a unique

"Color" that the providers or other cloud users can't detect.

The use of data coloring at varying security levels based on the variable cost function applied. This Progressive approach can also be applied to protect documents, images, videos, software, and relational databases in the cloud. The figure shows the details involved in the color-matching process, which aims to associate a colored data object with its owner, whose user identification is also colored with the same *Ex*, *En*, and *He* identification characteristics. The color-matching process assures that colors applied to user identification match the data colors. This can initiate various trust-management events, including authentication and authorization. Combining secure data storage and data coloring, the data objects can be prevented from being damaged, stolen, altered, or deleted . Thus, legitimate users have sole access to their desired data objects. The computational complexity of the three data characteristics is much lower than that performed in conventional encryption and decryption calculation.. The watermark-based scheme thus incurs a very low overhead in the coloring and decoloring processes. The *En* and *He* functions' randomness guarantees data owner privacy. These characteristics can uniquely distinguish different data objects.

PROPOSED SYSTEM

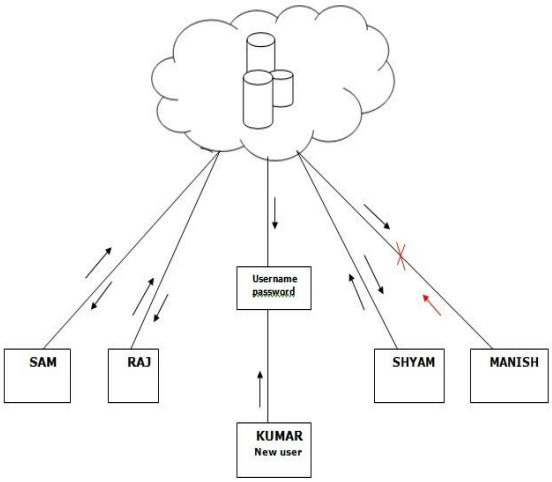
The problem with the existing system is no guarantee that only the legitimate users are accessing the confidential information in the cloud. When a legitimate user completes the one-time authentication the cloud service provider (CSP) does not worry about only the legitimate users, accessing the confidential information till the data user quits eventhough the data is secured with cloud drops. Hence to avoid this problem a

periodic authentication is proposed, guaranteeing that only legitimate users are in cloud till the end of the accessing period.

PERIODIC AUTHENTICATION

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 to 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.



A tiny bit of data may be sent to all the users who are accessing the data in the cloud after completing the one-time authentication, the user hash it with the unique individual key which is a negotiated value called entropy value and send the MAC (Message Authentication Code) the resultant value back to the server. The server on the other side hashes the same tiny bit of data, computes the same MAC value and compares the same with the users MAC. The SHA-1 hashing mechanism is used to hash the tiny bits which is irreversible whereas only comparisons can be made with the result. SHA-1 produce the 160-bit hash value. Original SHA (or SHA-0) also produce 160-bit hash value, but SHA-0 has been withdrawn by the NSA shortly after publication and was outdated by the revised version commonly referred to as SHA-1. The other functions of SHA series produce 224-, 256-, 384- and 512-bit hash values.The MAC value will be different to each user since all the entropy values are unique and easy to identify the identity of the user.

If both the values are same, it shows that only the legitimate user is accessing the confidential data since, the entropy value which is unique to everyone and knows only to the CSPs and user.

If the values are different, the server comes to know that there is a breach in the cloud and so the communication with the particular user is terminated.

CONCLUSION

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 which ensure that the legitimate user are accessing the data till he/she quits.

With an strong hashing algorithm (SHA-1), the hash is done and the results are compared for extending the access permission to the data in the cloud.

In future this periodic authentication can be made user driven where if any of the cloud user joins or leaves the cloud a new value of entropy is generated and the same periodic authentication can be made instead time intervals.

REFERENCES

1. Kai Hwang “Trusted Cloud Computing with Secure Resources and Data Coloring” Volume: 14, Issue: 5, IEEE Sept 2010.
2. 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.

3. 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.
4. Feng Zhu, Wei Zhu, Matt W. Mutka, "Private and Secure Service Discovery via Progressive and ProbabilisticExposure" VOL. 18, NO. 11, IEEE November 2008.
5. R. Zhou, and K. Hwang, "Power Trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, Apr. 2007, pp. 460–473.
6. E. Michail, A.P. Kakarountas, A. Milidonis, "Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 Hash function"©2004 IEEE.