2016 International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing, Networking and Communications (CNC)

Robust Scheme to Protect Authentication Code of Message/Image Documents in Cloud Computing

Zaid Ameen Abduljabbar[1,2], Hai Jin[1], Ali A.Yassin[2], Zaid Alaa Hussien[1,3],
Mohammed Abdulridha Hussain[1,2], Salah H. Abbdal[1], Deqing Zou[1]
[1]Cluster and Grid Computing Lab, Services Computing Technology and System Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
Email: zaidalsulami@yahoo.com, hjin@hust.edu.cn
[2]University of Basrah, Basrah, Iraq
[3]Southern Technical University, Basrah, Iraq

***Abstract*—A number of image/message document authentication and integrity schemes have been conducted to recognize any modification in the exchange of documents between two entities (sender and receiver) within a cloud environment. Existing solutions are based on combining key-based hash function with traditional factors (steganography, smart-card, timestamp). However, none of the proposed schemes appear to be sufficiently designed as a secure scheme to prevent common forms of attack such as replay, forgery, stolen verifier, brute force, and insider attacks. In this paper, we propose a scheme to ensure message/image document integrity for each user's login by providing one-time biometric message/image authentication code called *MACLESS*, which is a summation of combining the key-based hash function (MAC-SHA-1) of a message/image document and the one-time bio-key. Thereafter, *MACLESS* is hidden in a cover image based steganography anonymity. The proposed scheme has several important security attributes, such as phase key agreement, users' one-time bio-key, and one-time authentication code is valid only for one user's login session. Finally, security analysis and experimental results demonstrate and prove the invulnerability and efficiency of the proposed scheme.**

***Keywords*—Cloud Computing; MACLESS; One-Time Bio-key; One-Time Message/Image Document Authentication Code**

I. Introduction

Nowadays, transmitted information has radically increased and has been exponentially distributed [1]. Cloud computing is generally regarded as the computing infrastructure of the next generation; it is an effective means of enabling users to utilize large volumes of resources and provides an efficient and readily available on-demand service [2]. Consequently, users of cloud computing have raised information security requirements with regard to their communication compared with other challenges [3]. Message/image document integrity, and origin, which are achieved through communication between sender and receiver, have become huge security challenges. Different schemes based on key-based hash function to ensure message/image document authentication and integrity have been proposed. In [4-6], the authors proposed schemes that combining steganography approach with hashed value to transfer it securely. Most of those schemes used sequence mapping in the *least significant bits* (LSBs) of a cover-image to hide such value, which lacked in hiding efficiency and brought up a lot of security problems. Meanwhile, simply combining traditional factors (smart-card, timestamp, and shared key) with cryptographic hash function [7-11] are the most widely used methods to overcome security challenge and support data integrity routinely. These schemes still suffer from drawbacks related to such factors, thus these techniques might be vulnerable to common form of attacks. The probability of common attacks can be reduced by combining cryptographic hash function with a strong factor that should be periodically changed. For this reason, one-time authentication scheme [12, 13] can ensure the integrity and authentication, used one-time key to achieve such a goal.

In this paper, we report a scheme designed with a one-time bio-key. In details, the key used in the proposed scheme captures the advantages of a biometric technique that involves the use of the robust features extracted by the histogram of *local binary pattern* filter (LBP) [14] after combining the handwritten signature of the sender, the handwritten signature of the receiver, for generating one-time bio-key. This key is combining with MAC-SHA-1. The result of the combination is one-time message authentication code. Thereafter, the summation of such code called *MACLESS* is hidden in a cover image through LSBs [15] and *discrete wavelet transformation* (DWT) [15] based steganography anonymity. Concealing the anonymity of *MACLESS* depends on the one-time random pixel sequences generated by *Rivest Cipher 4* (RC4) [16] based on a one-time biometric stego-key. Although, a cloud service provider is needed in the proposed scheme, such provider in our scheme does not provide service in run time, but only in configuration phase.

The contributions of this paper: First, the proposed scheme provides one-time biometric message/image document authentication code between two parties in a cloud environment. Second, both service providers and users can achieve authenticated phase keys. Third, this scheme can provide biometric key management. Fourth, this scheme is computationally efficient and provides simple integration with the available infrastructure. Lastly, this scheme is effective against many attacks, as proven in the security analysis in Section III.

This paper is organized as follows. In Section II, the proposed scheme is described in terms of the configuration and verification phases. Section III presents a security analysis. Section IV provides system evaluation. Section V presents the conclusions.

978-1-4673-8579-4/16/$31.00 ©2016 IEEE