Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud

Mustafa A. Al Sibahee[1,2], Songfeng Lu[*,1,3], Zaid Ameen Abduljabbar[4,3,5,6], Erasmus(Xin Liu)[6], Yanli Ran[7],
Ahmed Abdulelah Jasim Al-ashoor[4], Mohammed Abdulridha Hussain[4,5,6], Zaid Alaa Hussien[8,6]
[1]Shenzhen Institute of Huazhong University of Science and Technology, Shenzhen, China
[2]Iraq University College, Basrah, Iraq
[3]Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering,
Huazhong University of Science and Technology, Wuhan, 430074, China
[4]University of Basrah, Basrah, Iraq
[5]Al-Kinoouze University College, Basrah, Iraq
[6]Neusoft Institute Guangdong, Guangdong, China
[7]Shenzhen University, Shenzhen, China
[8]Southern Technical University, Basrah, Iraq
Email: I201522098@alumni.hust.edu.cn, lusongfeng@hust.edu.cn
*Corresponding author: Songfeng Lu

***Abstract*—Document integrity and origin for E2E S2S in IoT-cloud have recently received considerable attention because of their importance in the real-world fields. Maintaining integrity could protect decisions made based on these message/image documents. Authentication and integrity solutions have been conducted to recognise or protect any modification in the exchange of documents between E2E S2S (smart-to-smart). However, none of the proposed schemes appear to be sufficiently designed as a secure scheme to prevent known attacks or applicable to smart devices. We propose a robust scheme that aims to protect the integrity of documents for each users session by integrating HMAC-SHA-256, handwritten feature extraction using a local binary pattern, one-time random pixel sequence based on RC4 to randomly hide authentication codes using LSB. The proposed scheme can provide users with one-time bio-key, robust message anonymity and a disappearing authentication code that does not draw the attention of eavesdroppers. Thus, the scheme improves the data integrity for a users messages/image documents, phase key agreement, bio-key management and a one-time message/image document code for each users session. The concept of stego-anonymity is also introduced to provide additional security to cover a hashed value. Finally, security analysis and experimental results demonstrate and prove the invulnerability and efficiency of the proposed scheme.**

***Keywords*—IoTs-Cloud; E2E S2S; Handwritten Signature; Bio-MAC.**

I. Introduction

At present, data transmission is increasing daily in an unprecedented way, especially with the increase in smart devices for the Internet of Things (IoT) [1]. Cloud computing is the most promising technology in providing an infrastructure for providing resources to users in terms of storage and processing anytime and anywhere [2]. At the same time, the IoT has a considerable effect on modern life, but it lacks the resources provided by cloud computing [3]. Thus, combining cloud computing and the IoT is necessary to make users enjoy the availability of resources and on-demand services.

Given the increasing number of forged and manipulated message/image documents, security and integrity have become primary concerns for enterprises, such as those in medicine, the military, e-government and e-commerce. Thus, these organisations have begun to search for methods that maintain integrity and authenticity to protect decisions made based on these message/image documents. Message/image document integrity, security and origin, which are achieved through smart devices users for E2E communication in IoT-cloud, have become huge security challenges. Different techniques to ensure data authentication and integrity have been proposed and are already being applied. Cryptographic one-way hash function and steganography [4, 10] are the most widely used methods to overcome this challenge and support data integrity routinely. However, MAC, disappearing data and combining simple factors with MAC are insufficient in maintaining the integrity of transferring message/image documents between E2E S2S over an unsecure communication channel. These techniques are vulnerable to replay and MITN attacks [9]. A highly secure and efficient scheme is needed for transferring sender message/image documents to the receiver over an unsecure communication channel while minimising the threat of attackers is yet to be established to address this issue.

To overcome the aforementioned disadvantages and develop a scheme that is capable of simultaneously providing integrity and authentication to message/image documents, a robust scheme that combines the biometric features extracted from a handwritten signature, HMAC-SHA-256 as authentication code and RC4 to generate one-time pixel sequence anonymity is proposed in this paper. Such a code is concealed through (LSB) steganography to establish advanced and robust one-time stego-anonymity between two parties and provide bio-key management that facilitates one-time anonymous message codes.

The main contributions of the proposed scheme to the IoT-cloud system is as follows. First, the proposed scheme addresses all previous weaknesses and thus presents a new ro-

978-1-7281-7202-6/20/$31.00 ©2020 IEEE