Received November 20, 2020, accepted November 23, 2020, date of publication December 1, 2020,
date of current version December 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041809

Lightweight Secure Message Delivery for E2E S2S Communication in the IoT-Cloud System

MUSTAFA A. AL SIBAHEE[1,2], **SONGFENG LU**[1,3], **ZAID AMEEN ABDULJABBAR**[3,4,5], **XIN LIU**[5], **HEMN BARZAN ABDALLA**[6], **MOHAMMED ABDULRIDHA HUSSAIN**[4,5], **ZAID ALAA HUSSIEN**[5,7], **AND MUDHAFAR JALIL JASSIM GHRABAT**[3]

[1]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 430076, China
[2]Department of Communication Engineering, Iraq University College, Basrah 61001, 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]Computer Science Department, College of Education for Pure Science, University of Basrah, Basrah 61004, Iraq
[5]Neusoft Institute Guangdong, Guangdong 528225, China
[6]School of Computer Science, Wenzhou-Kean University, Wenzhou 325060, China
[7]Information Technology Department, Management Technical College, Southern Technical University, Basrah 61001, Iraq

Corresponding author: Songfeng Lu (lusongfeng@hust.edu.cn)

This work was supported by the Hubei Provincinal Science and Technology Major Project of China under Grant No. 2020AEA011 and the Key Research & Development Plan of Hubei Province of China under Grant No. 2020BAB100. This work was also supported by the Science and Technology Program of Shenzhen of China under Grant No. JCYJ20180306124612893 and JCYJ20170818160208570.

ABSTRACT The continuous increase in the use of smart devices and the need for E2E smart2smart (S2S) services in IoT systems play effective and contemporary roles in the field of communication, and a large amount of resources is required. Thus, IoTs and cloud computing must be integrated. One of the results of this integration is the increase in the number of attacks and vulnerabilities in the E2E S2S message delivery service of such an IoT-cloud system. However, none of the traditional security solutions can be sufficiently regarded as a secure and lightweight mechanism for ensuring that the security requirements for E2E S2S message transmission in the IoT-cloud system are fulfilled. This work aims to provide an efficient and secure, lightweight E2E S2S message delivery function, which includes the E2E S2S secure key and biometric parameter exchange function, a bio-shared parameter and bio-key generation function, secure lightweight E2E S2S communication negotiation and secure E2E S2S lightweight message delivery. The secure, lightweight cryptographic communication procedure is negotiated between a pair of smart devices during each E2E session to minimize the power consumption required of limited-energy devices. Such a negotiation process prevents known attacks by providing responsive mutual authentication. Lightweight message delivery by the two smart devices can satisfy the basic security requirements of E2E communication and ensure that the computational cost required for a real-time system is as low as possible.

INDEX TERMS Message delivery function, IoT-cloud system, smart devices, E2E S2S, mutual authentication.

I. INTRODUCTION

Cloud computing has revolutionized information technology and attracted extensive attention from the research community and leading companies [1]. Cloud computing can be considered a new generation of computing infrastructure; this technology enables users to use vast resources in terms of storage and processing provides quick access to available services on request [2]. The Internet of Things (IoTs) can affect changes in daily activities and behaviours [3]–[6]. An IoT system may suffer from problems related to available resources in terms of transmission, storage, and processing. Consequently, cloud computing and IoTs need to be interconnected physically or virtually for smart device users to maximize cloud computing services [7]. Cloud computing and IoT users face certain information security challenges and requirements with regard to communication [7].

Numerous smart devices are currently used, and these devices need to communicate with one another. E2E S2S communication is an important issue in the IoT-cloud

The associate editor coordinating the review of this manuscript and approving it for publication was Moayad Aloqaily.