Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment

Shobhan Mandal, Basudeb Bera, Anil Kumar Sutrala, Ashok Kumar Das, *Senior Member, IEEE*, Kim-Kwang Raymond Choo, *Senior Member, IEEE*, and Youngho Park, *Member, IEEE*

***Abstract*—User access control is a crucial requirement in any Internet of Things (IoT) deployment, as it allows one to provide authorization, authentication, and revocation of a registered legitimate user to access real-time information and/or service directly from the IoT devices. To complement the existing literature, we design a new three-factor certificateless-signcryption-based user access control for the IoT environment (CSUAC-IoT). Specifically, in our scheme, a user U's password, personal biometrics, and mobile device are used as the three authentication factors. By executing the login and access control phase of CSUAC-IoT, a registered user (U) and a designated smart device (S_i) can authorize and authenticate mutually via the trusted gateway node (GN) in a particular cell of the IoT environment. In our setting, the environment is partitioned into disjoint cells, and each cell will contain a certain number of IoT devices along with a GN. With the established session key between U and S_i, both entities can then communicate securely. In addition, CSUAC-IoT supports new IoT devices deployment, user revocation, and password/biometric update functionality features. We prove the security of CSUAC-IoT under the real-or-random (ROR) model, and demonstrate that it can resist several common attacks found in a typical IoT environment using the AVISPA tool. A comparative analysis also reveals that CSUAC-IoT achieves better tradeoff for security and functionality, and computational and communication costs, in comparison to five other competing approaches.**

***Index Terms*—Automated validation of Internet security protocols and application (AVISPA), Internet of Things (IoT), key agreement, security, signcryption, user access control.**

Manuscript received October 30, 2019; revised December 28, 2019; accepted January 9, 2020. Date of publication January 13, 2020; date of current version April 14, 2020. This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Science, ICT, and Future Planning under Grant 2017R1A2B1002147; and in part by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India. The work of Kim-Kwang Raymond Choo was supported by the National Science Foundation (NSF) Centers of Research Excellence in Science and Technology (CREST) under Grant HRD-1736209. *(Corresponding author: Kim-Kwang Raymond Choo.)*

Shobhan Mandal is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India, and also with Huawei Technologies, Bengaluru, India (e-mail: shobhan.mandal@students.iiit.ac.in).

Basudeb Bera and Ashok Kumar Das are with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: basudeb.bera@research.iiit.ac.in; iitkgp.akdas@gmail.com).

Anil Kumar Sutrala is with CA Technologies—A Broadcom Company, Hyderabad 500 032, India (e-mail: anilkumarsutrala@gmail.com).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Youngho Park is with the School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea (e-mail: parkyh@knu.ac.kr).

Digital Object Identifier 10.1109/JIOT.2020.2966242

I. Introduction

IN AN Internet of Things (IoT) environment, Internet-connected devices are increasingly *smart* in the sense that most actions (e.g., collecting environmental data, which are then sent to the edge or cloud servers) are undertaken with minimal human intervention. These things are also called IoT devices and smart devices/objects, and can be either physical or virtual. Examples of such devices include cameras, sensors, smartphones, unmanned ground vehicles, and unmanned aerial vehicles (also referred to as drones). In a typical IoT environment, several smart devices are installed or deployed in a certain deployment area (e.g., smart home, smart city, and hospitals) that can sense relevant information from the surrounding area, and the sensed information is then disseminated to their respective gateway nodes (GNs). The smart devices are assigned with their unique identities, such as device ID or IP address. In recent times, there has been a trend to adopt IPv6 over low-power wireless personal area networks (6LoWPANs) in IoT settings [1], in order to deal with the increasing scale of deployment. For example, a study by Gartner Inc. [2] predicted that the number of connected IoT smart devices will be close to 20.4 billion and hardware spending from both cross-industry and vertical-specific IoT devices will be $3 trillion by the year 2020.

There are a number of challenges in setting up an IoT environment, and one particular example is security. For example, communications among various users, smart devices, and GNs typically take place over insecure channels. In other words, there is a risk that the communications can be intercepted, hijacked, deleted, modified (e.g., inserting fabricated messages), and so on. This necessitates the design and implementation of the secure and efficient user access control mechanism in the IoT system, in order to ensure that only authorized registered users are allowed access to the relevant information and/or services. As we will point out later in Section III, designing secure and efficient user access control solutions remain challenging.

In this article, we design a new three-factor certificateless-signcryption-based user access control scheme for an IoT environment (hereafter referred to as CSUAC-IoT). CSUAC-IoT permits a legitimate registered user U to access real-time data/services from a designated IoT smart device S_i, provided that mutual authentication is successful. The mutual authentication is carried out via the trusted GN. The session key established after mutual authentication is