








Multi-factor Authentication for an Administrator's Devices in an IoT Environment

Abdulla J. Y. Aldarwish¹  , Ali A. Yassin¹ , Abdullah Mohammed Rashid¹ ,
Aqeel A. Yaseen² , Hamid Alasadi¹, and Ahmed A. Alkadhmaewee¹

¹ University of Basrah, Basrah, Iraq

abdullajas@gmail.com, aliadel79yassin@gmail.com,
abdalla_rshd@yahoo.com

² Al Kunooz University College Computer Engineering Techniques, Basrah, Iraq
aay.ali80@gmail.com

Abstract. In the information technology era, authentication systems have been developed that use multi-factor authentication to ensure the authorisation of users and administrators. There are many schemes based on factors such as smart cards, biometrics, and token devices. Although these schemes are generally strong, they suffer from several drawbacks such as malicious attacks, factors that may be lost/stolen, and a need for extra hardware/software. In this paper, we propose a strong authentication scheme for an IoT environment to authenticate the owners of devices. Our work supports a negotiation service using an anonymous QR image as a second factor to check the authority of an administrator. The proposed scheme has good security features such as mutual authentication, a secure index file, anonymity of the user's identity and password, a secure session key, and perfect forward secrecy. Additionally, our work can resist well-known attacks such as the man in the middle, insider, and spoofing attacks, among others. In the real world, we apply our scheme using a mobile phone (Samsung Galaxy S5 model SM-900H) and server (Intel Xeon E3 – 1220LV2 3.5GHZ 4GB RAM). Based on its accuracy and performance standards, we obtain good results in the login and authentication phases. Moreover, the computational cost of our work is comparable to that of related works.

Keywords: QR image · MITM · IoT · Strong authentication · Mobile phone

1 Introduction

The Internet of Things (IoT) offers an ideal model for future communication networks and can facilitate the use of the internet for all things related to civil society, based on rapid technological development. The components of this network are physical objects, sensors, triggers, RFID tags, and mobile devices that have the ability to sense and control the environment remotely and to collect the necessary data associated with the user's environment, for example in smart companies and smart homes [1, 2]. The collected data