Acta Scientific COMPUTER SCIENCES

Volume 2 Issue 10 October 2020

Editorial

Biometric Authentication: An Efficient Option for Internet of Things Applications During the COVID-19 Pandemic

Shahram Babaie*

Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

***Corresponding Author:** Shahram Babaie, Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran.

Received: August 24, 2020
Published: September 01, 2020

The Internet of Thing (IoT) as an emerging technology is a platform of interrelated devices, inanimate and animate entities that are equipped with Unique IDentifiers (UIDs), which can transfer data through Device-to-Device (D2D) and Machine-to-Machine (M2M) protocols. This technology enables companies to automate processes and reduce labor costs. IoT also cuts down waste and makes the production and delivery of goods cheaper, as well as providing transparency to customer transactions. In financial and e-health applications, IoT devices can access to sensitive personal and banking information, which motivates hackers to steal this information. Likewise, since IoT elements typically communicate with each other via wireless channels, this technology is prone to various attacks such as eavesdropping, man-in-the-middle, Sybil, and jamming.

In general, Confidentiality, Integrity, and Availability, which is known as the CIA triad, is a common model for security policy development. Confidentiality refers to actions that ensure sensitive information is only accessible to authorized entities, which can be achieved by authentication mechanisms. In general, an entity can be authenticated through three main factors, i.e. knowledge, possession, and inherence. In the knowledge factor, which refers to something the user knows, credentials such as Personal Identification Number (PIN), username and password, and answer of a secret question are used for authentication. The possession factor, which refers to something the user has, is based on the items that the user can own and carry, including hardware devices such as a security token and mobile phone to accept text messages and run an authentication application. In the inherence factor, which refers to something the user is, the biometric characteristics are used for authentication. In addition to the mentioned factors, location factor and time factor, which refer to where the user is and when the user is authenticating, respectively, can be applied for authentication. The Single-Factor Authentication (SFA) mechanisms that rely on just one credential category are not resistant to attacks, and Two-Factor Authentication (2FA) and Multifactor Authentication (MFA) approaches have been proposed to increase the authentication resilience.

Biometric authentication is entirely based on the measurement and statistical analysis of users' inherent physical and behavioral characteristics and provides unparalleled security benefits. In recent years, biometric-based verification has become increasingly popular in corporate security systems because it is easy, and no password is required to remember or carry security tokens. The biometric-based authentications are based on either physiological or behavioral characteristics. In general, physiological identifiers rely on facial recognition, fingerprints, finger geometry, iris recognition, vein recognition, retina scanning, and voice recognition. Whereas, behavioral-based identifiers rely on unique individual's acts, such as typing patterns, walking gait, and other gestures. The authentication is necessary for both remote-control and local-control applications of IoT. In remote-control applications, an end-user, such as a physician or homeowner, issues the necessary commands after receiving reports and monitoring events. In local-control applications, the users must be verified before accessing a place or resource through a smart gate and IoT-enabled vehicle. Biometric-based authentication is growing due to its inherent benefits such as ease of use and convenience, hard to fake or steal, little changes over the user's life, non-transferable, and need for fewer storage patterns. In addition to the mentioned benefits, biometric authentication can dramatically reduce the likelihood of Coronavirus spreading in IoT-based applications. So that any kind of touchless and contactless sensors and detection equipment is an effective way to deal with the COVID-19 pandemic. It should be noted that as soon as the Coronavirus spread, active IoT companies have begun extensive efforts to combat it. Therefore, it is evident that IoT-based thermal scanning and intelligent monitoring of patients reduce the risk of COVID-19. Undoubtedly, improving human health and welfare is a common goal of technology and the IoT. It can be concluded that biometric authentication is a valuable assistant for technology in the days when Coronavirus has caused serious problems for human health.