A Simulation System Using the Internet of Things for Sevrity Sensing Services

Ali Tariq Kalil Al-Khayyat

Department of Electrical and Computer Engineering, Institute of Graduate Studies, Altınbaş University, Istanbul, Turkey

Department of Dental Basic Sciences, College of Dentistry, University of Mosul, Mosul, Iraq

Seyfi Yildiz

Department of Electrical and Computer Engineering, School of Engineering and Architecture, Altınbaş University, Istanbul, Turkey

Osman Nuri Ucan

Department of Electrical and Computer Engineering, School of Engineering and Architecture, Altınbaş University, Istanbul, Turkey

Abstract:

IoT security has become very important in recent days because of the increase in applications and areas that can be used where the security of information is an important issue. In this work, a proposed system has been designed to secure communication between the client and the IoT device. The proposed system utilizes two strong security techniques, steganography and cryptography. The proposed system has taken advantage of these technologies where encryption protects the main authentication information as well as the IoT communication port and changes it to an unreadable form (Ciphertext), then embedding this Ciphertext within stego message to trick the observer there is any existing to the original message and prevent any suspension there is encryption in data. The overall test shows that this proposed method is very strong from a security point of view, and the operation test shows it works efficiently without any problem it fast takes about 2.5 seconds and is low in size which makes it useful even with low-speed internet. The main advantage is that no information can be obtained without passes successfully from all security strategies, which require first knowing if there is stego message, need to know which stego method is used, need to know which list is, need to know the encryption algorithm, the crypto key, and to have same mac that used in encryption. This is very hard and can say it is impossible to crack no one can connect an even know the IoT IP address without having the overall parts after that there is a need to right authentication information for IoT things.

Keywords:

IOT, security, steganography, stego, cryptography, AES, HMAC.