Towards secure IoT-based payments by extension of payment card industry data security standard (PCI DSS)

ABSTRACT

IoT emergence has given rise to a new digital experience of payment transactions where physical objects like refrigerators, cars, and wearables will make payments. These physical objects will be storing the cardholder credentials and will directly make payments with the vendors over insecure public networks. For such payment transactions, government regulations and standards organizations require to implement PCI DSS for adapting similar set of security measures at the global level. The current version of PCI DSS is not suitable for IoT-based payment systems due to characteristics of IoT such as resourceconstrained nature of devices and updating software/firmware of so many physical devices. Also, there arises an emergent need of implementing PCI DSS requirements and assessments for security of all stakeholders that store or process the user credentials in a payment. This paper is an initial effort to bring the researcher's attention to make upcoming versions of PCI DSS suitable for IoT and thus securing the new ways of IoT-based payment systems. The paper has reviewed the traditional payment process along with considerations for IoT-based payment systems to make recommendations to modify the PCI DSS in a suitable way for IoT.