Securing mhealth applications with grid-based honey encryption

ABSTRACT

Mobile healthcare (mHealth) application and technologies have promised their cost-effectiveness to enhance healthcare quality, particularly in rural areas. However, the increased security incidents and leakage of patient data raise the concerns to address security risks and privacy issues of mhealth applications urgently. While recent mobile health applications that rely on password-based authentication cannot withstand password guessing and cracking attacks, several countermeasures such as One-Time Password (OTP), gridbased password, and biometric authentication have recently been implemented to protect mobile health applications. These countermeasures, however, can be thwarted by brute force attacks, man-in-the-middle attacks and persistent malware attacks. This paper proposed grid-based honey encryption by hybridising honey encryption with grid-based authentication. Compared to recent honey encryption limited in the hardening password attacks process, the proposed grid-based honey encryption can be further employed against shoulder surfing, smudge and replay attacks. Instead of rejecting access as a recent security defence mechanism in mobile healthcare applications, the proposed Grid-based Honey Encryption creates an indistinct counterfeit patient's record closely resembling the real patients' records in light of each off-base speculation legitimate password.