Dr.SENTHIL PRABHA R

ABSTRACT

CERTAIN INVESTIGATIONS ON TOUCH DYNAMICS FOR USER AUTHENTICATION ON TOUCH SCREEN MOBILE DEVICES

Mobile devices like smart phones and Personal Digital Assistants (PDA) play an increasingly important role in the digital environment. The devices are equipped with applications that are geared to store sensitive data in addition to the standard contacts, tasks and scheduling utilities. The invariable applications of these devices brings new security and privacy risks. In addition, when the devices are used continuously, the users tend to leave the traces of their identities and transactions. Hence, user authentication plays a vital role. Authentication is a process to identify individuals and verify their eligibility to access a system or a device in a secured manner. It is a security measure designed to protect any system against imposters.Methods for authentication are generally classified into three categories.(1) Techniques based on passwords, pin codes and passphrases, (2) Techniques based on one-time passwords (OTPs), (3) Techniques using unique features of a human body like the physiological features or the behavioural characteristics. Though, these technologies provide different levels of security, none has been proven to secure the system completely.

While deploying biometrics for user authentication, it demands either an identification process or verification process before providing access privileges to the user. Based on the application, authentication isof two categories namely: static authentication and continuous authentication. Static authentication verifies the identity before entering a system, whereas continuous authentication verifies the identity even after the user has entered into the system.

The thesis investigates the possibilities of providing touch dynamic authentication solutions can be applied to real time environments. To authenticate the user, touch dynamic features are extracted while interacting with traditional authentication mechanisms. Verification is based on both the pattern exhibited and the touch dynamics.

The first chapter provides an introduction to authentication and the need for authentication. It analyses various types of available authentication mechanisms. Also this chapter specifies the need for this proposed research in the context of existing approaches. Second chapter surveys the prior work and positions the contribution of this research in the

context of existing approaches. Researchers have used various classification methods for biometric user authentication.

Few classification methods adopted for this research work and the performance evaluation are also detailed in this chapter.Feasibility of the touch dynamic PIN based authentication technique is investigated in the third chapter. The fourth chapter explores the benefits of graphical passwords for user authentication. It adopts recognition based graphical passwords and the work takes cognizance of the user's tapping behaviour in selecting the sequence of images for the purpose of authentication.

Fifth chapter proposes a touch dynamic lock pattern technique. Touch dynamic lock pattern is the pattern, that the user exhibits by traversing on an 'n x n' grid of points displayed on the touch screen. The value of 'n' is usually 3 or 4. Since more number of derived features such as maximum recorded speed and minimum recorded speed are considered, to better represent the user pattern. A feature reduction technique is adopted to improve the accuracy of the authentication system.

The sixth chapter details the swipe based authentication technique. The results conclude that the touch dynamic swipe pattern authentication technique enhances the usability and security. Suitability of feature reduction is also analyzed by conducting tests on a reduced feature set. Touch dynamic continuous authentication (CA) is proposed in the seventh chapter to determine the possibility of identifying the user in continuous environments.

The possibility of authenticating the user based on their activity pattern while engaging in traditional authentication techniques is explored. A framework to authenticate users while they perform the operations continuously is established. A model is built to provide authentication throughout the entire session of interaction. Eigth chapter consolidates the result findings of user authentication using touch dynamics and few further research directions are suggested in ninth chapter.