Oral presentation: 263

Modeling a user authentication & verification protocol for web applications using keystroke dynamics

D. T. S. Kasun* and B. Jayawardane

Department of Industrial Management, Faculty of Science, University of Kelaniya, Sri Lanka
*shiranthakasun@yahoo.com

With the advent of new technologies which surpass their predecessors, the impact of information on the lives of people has immensely proliferated. In this challenging and dynamic environment, the need for reliable computer security steadily increases. Biometric technologies are used widely to ensure the security aspect of a system. They are divided into two categories as physical biometrics and behavioral biometrics. Physical biometrics are based on direct measurement of various parts of the human body while behavioral biometrics are related to the behavior exhibited by people. Modern systems mostly do the authentication in the user login phase. In this phase, authenticating a user with a username and a password is done. This is named as the static authentication. There are also some systems that do the authentication passively when the user is working in the session. This is called the continuous authentication. In both types of authentication processes, we can utilize keystroke dynamics for user authentication. It is a behavioral biometric which concern about the typing pattern of a user. The objective of this research is to develop a secure user authentication and verification model for web applications using keystroke dynamics based on the time dimension which includes static authentication for user authentication and continuous authentication for user verification. The time factor will be considered in building this model since the way a person types can be different in various occasions due to various circumstances. Studying the previous work done related to keystroke dynamics in the behavioral biometrics domain was completed at the beginning of this research. Various measures such as dwell time and flight time used in previous works were considered when selecting most suitable measures used in keystroke dynamics. In the second phase of the research, development of the machine learning model will be done. The incorporation of suitable measures into the model using the machine learning technique selected will be done in this stage. In the final stage of the research, validation of the construction model will be done. An optimum population for validation should be selected at the start of this stage. Through this validation, the accuracy of model developed can be assessed. This constructed model expected to be more accurate and sophisticated since it incorporates both static authentication and continuous authentication into a single system.

Keywords: Behavioural biometrics, keystroke dynamics, user authentication