Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.4, No.1, 2014

KeyStroke Dynamics - Dangling Issues of Providing Authentication by Recognising User Input

D. Ramya Krishna (Mtech)
Assistant Professor,
Vignan's Nirula Institute Of Technology & Science For Women.
D. Koteswaramma (Mtech)
Assistant Professor,
Vignan's Nirula Institute Of Technology & Science For Women.
* E-mail of the corresponding author: ramyakrishna28.dhulipalla@gmail.com

Abstract

A behavioral biometric such as keystroke dynamics which makes use of the typing cadence of an Individual can be used to strengthen existing security techniques effectively and cheaply. Due to the ballistic (semi-autonomous) nature of the typing behavior it is difficult to impersonate, making it useful as a biometric. Therefore in this paper, we provide a basic background of the behavioural basis behind the use of keystroke dynamics. We also discuss the data acquisition methods, approaches and the performance of the methods used by researchers on standard computer keyboards. In this survey, we find that the use and acceptance of this biometric could be increased by development of standardized databases, assignment of nomenclature for features, development of common data interchange formats, establishment of protocols for evaluating methods, and resolution of privacy issues.

Keywords: Authentication, Behavioural biometrics, Identification, keystroke dynamics, typing.

Introduction

For user authentication and identification in computer based applications, there is a need for simple, low-cost and unobtrusive device. A user can be defined as a person who attempts to access information stored on the computer or online using standard input device such as the keyboard. Use of biometrics such as face, fingerprints and signature requires additional tools to acquire the biometric which leads to an increase in costs. Use of a behavioral biometric which makes use of the typing pattern of an individual can be obtained using existing systems such as the standard keyboard, making it an inexpensive and extremely attractive technique. One of the major advantages of this biometric is that it is non-intrusive and can be applied covertly to augment existing cyber-security systems.

A biometric system can be divided into two categories based on the type of application – authentication and identification. Authentication is the process of determining whether someone is, in fact, who they claim to be. This authentication process is often categorized by the number of factors that they incorporate [25]:

1) something you know (e.g., a password),
2) something you have (e.g., token, certificate, ID badge etc.),
3) something you are (e.g., biometrics finger print, iris scan, etc.). A strong authentication is referred to a combination of two or three of these processes. On the other hand identification is the process of associating the person with an identity [76]. In this process, the system seeks to gain knowledge about the subject and associate it with either a set of pre-defined or unknown identities.

Behavioural biometrics depends on detecting the behavioural features of the user, such as signature, voice, and keystroke dynamics. Keystroke Dynamics is inexpensive to implement because typing pattern of an individual can be obtained using existing systems keyboard. In this paper we have clearly identified the work based on the Behavioural Characteristics of the user.

The behavioural biometric of Keystroke Dynamics is the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Raw measurements available from every keyboard can be recorded to determine Dwell time (the time a key pressed) and Flight time (the time

between"key up" and the next "key down"). Key hold time or dwell time is defined as the time for which each keystroke was pressed. The keystroke latency is the combination of the hold and flight times.In other words, the system verifies how a person types. Keystroke
verification techniques can be categorized as either static or continuous. Keystroke Dynamics Static verification system approaches study keystroke characteristics at a specific time. Continuous verification, on the other hand, examines the user's typing behavior , throughout the interaction time. Time-features can be extracted from keystroke data in many ways, such as studying keystroke latency, duration of key hold, pressure of keystroke, frequency of word errors, and typing rate. However, not all of these methods are widely used. Keystroke solutions are usually measured in three ways:
dwell time – how long a key is pressed, flight time – how long it takes to move from one key to another, and key code.
The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both identification and authentication tasks. Data needed to analyze keystroke dynamics is obtained
by keystroke logging.

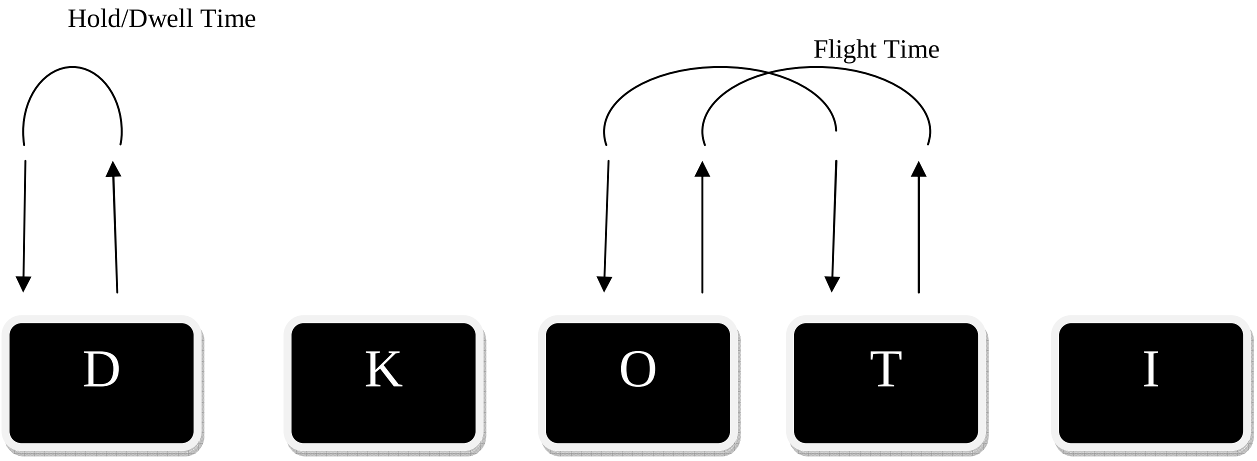

Figure 2: Keystroke Dynamics

Conclusion

A functional structure made up of holons is called holarchy. The holons, in coordination with the local environment, function as autonomous wholes in supra-ordination to their parts, while as dependent parts in subordination to their higher level controllers. When setting up the WOZIP, holonic attributes such as autonomy and cooperation must have been integrated into its relevant components. The computational scheme for WOZIP is novel as it makes use of several manufacturing parameters: utilisation, disturbance, and idleness. These variables were at first separately forecasted by means of exponential smoothing, and then conjointly formulated with two constant parameters, namely the number of machines and their maximum utilisation. As validated through mock-up data analysis, the practicability of WOZIP is encouraging and promising.

Suggested future works include developing a software package to facilitate the WOZIP data input and conversion processes, exploring the use of WOZIP in the other forms of labour-intensive manufacturing (e.g. flow-line production and work-cell assembly), and attaching a costing framework to determine the specific cost of each resource or to help minimise the aggregate cost of production.

References

Arai, T., Aiyama, Y., Sugi, M. & Ota, J. (2001), "Holonic Assembly System with Plug and Produce", *Computers in Industry* 46, Elsevier, 289-299.

Bell, G.A., Cooper, M.A., Kennedy, M. & Warwick, J. (2000), "The Development of the Holon Planning and Costing Framework for Higher Education Management", Technical Report, SBU-CISM-11-00, South Bank University, 103 Borough Road, London, SE1 0AA.

Bongaerts, L. (1998), "Integration of Scheduling and Control in Holonic Manufacturing Systems", *PhD Thesis*, PMA Division, K.U.Leuven.

Deen, S.M. (1993), "Cooperation Issues in Holonic Manufacturing Systems", *Proceedings of DIISM'93 Conference*, 410-412.

Techawiboonwong, A., Yenradeea, P. & Das, S. (2006). A Master Scheduling Model with Skilled and Unskilled Temporary Workers", *Production Economics* 103, Elsevier, 798-809.

Valckenaers, P., Van Brussel, H., Bongaerts, L. & Wyns, J. (1997), "Holonic Manufacturing Systems", *Integrated Computer Aided Engineering* 4(3), 191-201.

Van Brussel, H., Wyns, J., Valckenaers, P., Bongaerts, L. & Peters, P. (1998), "Reference Architecture for Holonic Manufacturing Systems: PROSA", *Computers in Industry* 37(3), 255-274.