PERSON IDENTIFICATION BY KEYSTROKE DYNAMICS USING PAIRWISE USER COUPLING

ABSTRACT

Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. **Keystroke dynamics** is a behavioral biometric, this means that the biometric factor is 'something you do'. Already during the Second World War a technique known as *The Fist of the Sender* was used by military intelligence to distinguish based on the rhythm whether a morse code message was send by ally or enemy. These days each household has at least one computer keyboard, making keystroke dynamics the easiest biometric solution to implement in terms of hardware.

EXISTING SYSTEM

Due to the increasing vulnerabilities in cyberspace, security alone is not enough to prevent a breach, but cyber forensics or cyber intelligence is also required to prevent future attacks or to identify the potential attacker. In most cases, it is important to detect that the current user is not the authenticated user, for example in the event of PC hijacking, where the information on a system is protected against unauthorized access or modification. Another case could be an online exam where there needs to be certainty that the student behind the keyboard is, in fact, the one that should be taking the exam. In some cases, it could also be interesting to not only authenticate the current user but also maybe to identify him or her. In the previous example of the online exam, in case fraud is detected when the authentication module detects that the student was typing the exam is not the intended student, it could be interesting to identify this person because it could be one of the current or previous students that already has passed the exam. Another situation where identification could be useful is in an online closed or open user forum. Here it could be used to identify the person posting an anonymous yet offensive or criminal comment, or posting a comment under the name of another person, e.g. after getting

access to the account of the other person. Finally, an example where identification could be of use is in a chat room, where the behaviour of an unknown person is compared to the known profiles. For example, if a person is showing pedophile behavior, then his or her typing behaviour can be compared to the behaviour of a set of known pedophiles.

Disadvantages

- Information on a system is not protected against unauthorized access or modification.
- Cannot identify a person based on the person's typing behavior.

PROPOSED SYSTEM

In our proposed system, we will explore the potential of KD for person identification. We will focus on classification techniques with different KD features for identification. We will also study the effect of user handedness on the accuracy of identification. We propose three different identification schemes in this paper. These schemes are based on the pairwise user coupling, where the multi-class pattern identification problem will be divided into several two-class problems. These schemes could be useful for person identification when the biometric features are weak, or there are few samples present for learning Extensive analysis was done with an online exam based keystroke datasets; This dataset was collected from 64 individuals with three different typing modes. To validate our research approach furthermore we have used another keystroke dynamics dataset with our optimum settings. All These datasets are publicly available for future research; We performed the analysis for both open-set and close-set settings and show that our optimum settings outperform the state of the art research.

Advantages

- Information on a system is protected against unauthorized access or modification.
- Identifying a person based on the person's typing behavior.

SOFTWARE REQUIREMENTS

Front-end : JSP

Back-End : MySQL

Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB