Chapter 56
Keystroke Dynamics: A Behavioral Biometric Model for User Authentication in Online Exams

Senthil Kumar A. V.
Hindusthan College of Arts and Science, India

Rathi M.
Dr. N. G. P. Arts and Science College, India

ABSTRACT

Online learning has entirely transformed the way of learning by the students. Online tests and quizzes play an important role in online learning, which provides accurate results to the instructor. But, the learners use different methods to cheat during online exams such as opening a browser to search for the answer or a document in the local drive, etc. They are not authenticated once they login and progress to attend the online exams. Different techniques are used in authenticating the students taking up the online exams such as audio or video surveillance systems, fingerprint, or iris recognition, etc. Keystroke dynamics-based authentication (KDA) method, a behavioral biometric-based authentication model has gained focus in authenticating the users. This chapter proposes the usage of KDA as a solution to user authentication in online exams and presents a detailed review on the processes of KDA, the factors that affect the performance of KDA, their applications in different domains, and a few keystroke dynamics-based datasets to authenticate the users during online exams.

INTRODUCTION

Authentication is the process to ensure an individual's identity. This provides access control for systems by verifying the user's credentials with the credentials stored in a database. Only authenticated users are allowed to access the protected resources of the organizations which are called as authorization process. The terms authentication and authorization are often used interchangeably; Authentication confirms the identity of a registered user before permitting access to the protected resource, whereas authorization confirms that the authenticated user has the permission to access the requested resources or not. Security

DOI: 10.4018/978-1-7998-8047-9.ch056

of the computers is compromised through unauthorized access of highly confidential information. User authentication is the primary method in preventing unauthorized access of information. It is generally classified into three categories. i) Knowledge Based Authentication (Something the user knows): User name and passwords is the best example for this method. This is very popular as it authenticates the user directly and it also does not require any special hardware for authentication. ii) Object Based Authentication (Something the user possesses): The users are identified by presenting or applying physical objects i.e. electronic chip cards, RFID tags etc. iii) Biometric Based Authentication (Something the user is): Identifying an individual based on his/her unique physiological and/or behavioral characteristics.

Now-a-days, the usage of hard copy of the book materials is getting reduced as purchasing the book is expensive and also it becomes outdated in the modern learning environment. The book materials reproduced and stored in another storage media may not help the users, as the device may become inaccessible at the time of requirement. But, online learning is an environment where these drawbacks could be overcome. The course contents can be uploaded online and the user can access them at any time. At the end of the course, the users are expected to undertake the exam online. Few users attend the exam genuinely and few others involve in forgery by asking some of their friends (an impostor) to take up the exam instead of them, so that they can score high. This acts as a great challenge to the one who is conducting the exam. Hence, it becomes important to authenticate the users during the entire session of the online exam. The most effective method of user authentication is based on biometrics. Keystroke Dynamics is a behavioural biometric authentication method which is used to authenticate the user during the online exams. This chapter presents the significance of online learning environment, literature review on the various biometric techniques that are applied to prevent cheating in online examination systems, and it particularly focuses on keystroke dynamics based authentication model, which has been used as a strong authentication model by the researchers. Applications of keystroke dynamics in different domains, the factors that affect the performance of the keystroke dynamics model have also been discussed.

BIOMETRIC TECHNOLOGIES: AN OVERVIEW

The following section discusses on the various biometric technologies available for authentication which are broadly categorized based on their physical characteristics or behavioural characteristics.

Physiological Biometrics

Physiological biometrics are those features that describe ‘who the user is’ depending on their physical attributes such as fingerprints, face, iris, retina scanning, hand geometry etc.

Facial Recognition

The most widespread biometric characteristic used by humans to make a personal identification is the facial recognition. It uses the spatial geometry of distinctive features of the face. It is a type of computer vision that uses the face to identify or to authenticate a person. It does not require any additional hardware, as it can be used with existing image capture devices like webcams, security cameras, etc. The features of a face include the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin etc. The face recognition software uses deep learning algorithms to compare live captured