**INTRODUCTION**

Identification has been a highly-valued research topic, as it involves every aspect of human life, from national security to unlocking personal accounts. At present, the main methods of identification are passwords and physical tokens like fingerprints and iris. However, with the development of artificial intelligence and machine learning, behavioral biometrics emerge as an alternative way of identification, and some voices claim that it outweighs the traditional methods. Nevertheless, it is clear that passwords and physical tokens “can easily be stolen or duplicated” and therefore are not the best way to ensure security. Despite fingerprints and iris “can sometimes be difficult to use”, they do have concrete merits. First, the datasets can be easily obtained by scanning a fingertip or an iris. Second, this data-collecting process usually takes less than a minute. Third, the sizes of the data are usually small enough for normal calculation and storage. These advantages together make fingerprints and iris the most widely used security measures across the globe. Compared to them, behavioral biometrics have not gained many advantages, let alone that some people may not wear smartwatches or put their phones in their pockets. One feature of behavioral biometrics is still notable though – it can carry out the identification processes through subjects' movements without many environmental requirements, and therefore make the process more convenient. Comprehensively speaking, to make this identification method stand out among its peers, we need to simplify the data collected, shorten the training time, and improve the accuracy of the model. Therefore, this essay will touch on these topics by proposing a new model used for behavioral biometrics.