Behavioral Analysis For a Continuous User Authentication

Giacomo Giorgi
Supervised by Fabio Martinelli and Andrea Saracino

Istituto di Informatica e Telematica-Consiglio Nazionale Delle Ricerche
{firstname.lastname}@iit.cnr.it

Abstract. New generation devices are pervasive in nature and provide a number of security sensitive functionalities, which might expose the user private information to serious security and privacy threats. The main countermeasure used to prevent unauthorized access is the user authentication. Most of these devices are still protected by traditional authentication mechanisms (PIN, password), which are exposed to well known security limitations. These issues are mitigated by the introduction of new physical biometric authentication mechanisms. Biometric authentication, basing on user physical traits and requiring the user presence at the authentication time, makes the system more secure. Despite the new mechanisms overcome some data security issues, they still suffer from other usability problems. In this paper we explore a new unobtrusive authentication mechanism based on human behavior.

Keywords: Machine learning · Authentication · Human behavior.

1 Introduction

The most common user authentication mechanisms used are based on the concepts of: (i) what the user knows, (ii) what the user has, (iii) what the user is, (iv) what the user does. The traditional authentication mechanisms (i, ii) as explained in literature [4] are not considered much safe to provide security to the users because of many flaws in the conventional systems. These security issues are mitigated by the introduction of the physical biometric authentication mechanisms. However the systems based on physical biometrics require more users cooperation since such traits cannot be analyzed unobtrusively, thereby reducing the usability of the system. The main open challenges of an authentication system are: (i) Identification of a discriminative biometric trait, (ii) Limited resource available, (iii) Robustness over biometric trait variation, (iv) unobtrusiveness. In this paper is described the structure of a new authentication mechanism based on the physical human behavior analysis exploiting the user interaction with its smart devices.

2 Related work

Use sensor data to identify and authenticate smartphone users based on a person's movements is a topic already treated in literature. In the paper [2], they collect individuals data related to walk, jog, and climb stairs having a mobile phone equipped with the sensor and they demonstrated to function as biometric signatures. In a similar way [3], demonstrated that the way a phone is held or kept at different positions through motions can be used to authenticate users.

3 Approach

The approach proposed in order to solve the aforementioned issues, is based on the aggregation of different behavioral analysis classified in: (i) behavioral user actions, (ii) user interactions with the smart devices and reported in Table 1. In

Action	behavioral user action	Device interaction
Free texting sitting/walking	x	v
Unlock from table/pocket/bag	x	v
Web page browsing	x	v
Walking up and down inclination ground	v	x
Running up and down inclination ground	v	x

Table 1. User's actions

order to avoid the direct user interaction with the system and make it less intrusive, data are collected transparently from the devices' sensors (accelerometer and gyroscope). Basing on the fact that each user can has a unique distinctive behavior in doing these actions, it is possible build a system ables to recognize a user starting from the analysis of its behavior. The system is composed by two main components: (i) Human Action Recognition (HAR), (ii) User verification. The HAR component performs the task of identifying the specific movement or action of a person based on sensor data, while the user verification component is used to verify the identity of who has performed the action. Figure 1 shows the complete pipeline.

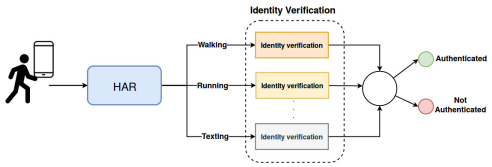

Fig. 1. Behavioral Authentication System

3.1 Implementation

As first step has been implemented an Android application ables to fetch data from the main smartphone sensors. The application requires to the user to perform the specific actions listed in Table 1 in order to catch sensors' values associated to the action required. The data collected will be used to train a Human Action Recognition in recognizing the new type of actions defined. The *Identity verification* component, as showed in Figure 1 is composed by a set of sub components, each of one dedicated to the verification of the identity through the analysis of a different action. One of the sub component analyzed is the *Gait recognition component*. As explained in the paper [1] a deep neural network

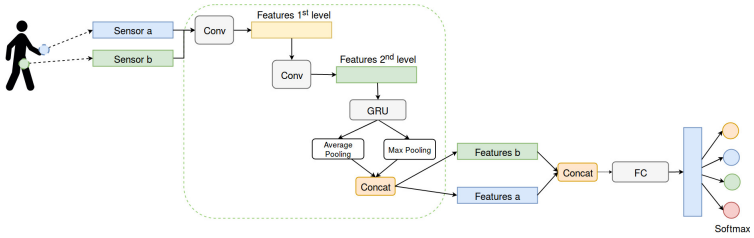

Fig. 2. Gait recognition architecture

architecture is applied to the problem on identifying 153 person exploiting 2 inertial sensors located on the right wrist and on right side of pelvis. Given a gait cycle (walking cycle that starts with initial contact of the right heel and it continues until the right heel contacts the ground again), the task is to determine to which person the cycle belongs. The network extracts, from a single input gait cycle, features of two different abstraction level (through two 1D convolutional layers) and applies a temporal aggregation on the features extracted in the second level (bidirectional recurrent layers). The result is a temporal aggregation feature vectors that are concatenated and passed to a fully connected layer composed by 153 softmax units which compute the probability of the input gait cycle to belong to a specific identity. Figure 2 shows the architecture.

4 Experiments

The experiments are done on the ZJU-gaitAcc dataset that is described in [5]. The dataset contains the gait acceleration series of records collected from 153 subjects gathered in two walking sessions. The aim of our experiments is to learn user identity starting from its walking path. To this end we considered two scenarios in which we experimented the recognition ability in the same session (walking gaits recorded in the same day) and in different sessions (walking gaits recorded over time). Figures 3 and 4, show the CMC curve reporting the

recognition accuracy for both scenarios. The real case, right side of the pelvis-right wrist (S3-S1), reaches 94% and 96% of accuracy at rank-1 respectively in cross sessions and single session scenario.

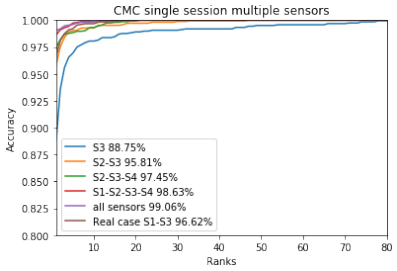

Fig. 3. CMC curve single session

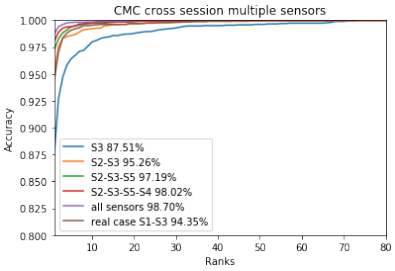

Fig. 4. CMC curve cross session

5 Conclusion and Future work

As showed in Section 3.1, the gait identification network reaches an high accuracy in recognizing a person among 153 different identities, that result is very promising in perspective of the implementation of a verification network. As future work, starting from the gait identification network, we plan to implement a siamese architecture to better adapt to verification problem. In addition we plan to reproduce the experiments on the data collected through smartphone and finally extend the verification to other user actions in combination with a HAR based on the actions showed in Table 1.

References

1. Giorgi, G., Martinelli, F., Saracino, A., Sheikhalishahi, M.: Walking through the deep: Gait analysis for user authentication through deep learning. In: IFIP International Conference on ICT Systems Security and Privacy Protection. pp. 62–76. Springer (2018)
2. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). pp. 1–7. IEEE (2010)
3. Primo, A., Phoha, V.V., Kumar, R., Serwadda, A.: Context-aware active authentication using smartphone accelerometer measurements. In: Proceedings of the IEEE conference on computer vision and pattern recognition workshops. pp. 98–105 (2014)
4. Raza, M., Iqbal, M., Sharif, M., Haider, W.: A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal **19**(4), 439–444 (2012)
5. Zhang, Y., Pan, G., Jia, K., Lu, M., Wang, Y., Wu, Z.: Accelerometer-based gait recognition by sparse representation of signature points with clusters. IEEE transactions on cybernetics **45**(9), 1864–1875 (2014)