BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 1. SZÁM

Biometrics acquisition in a Hungarian university
The Óbuda University case - Bánki Donát Faculty

Huu Phuoc Dai Nguyen[1,2], Lourdes Ruiz[1], Arnod Őszi[1]

[1]Doctoral School on safety and security sciences, Bánki Donát, Óbuda University
Budapest, Hungary
[2]CanTho Technical Economics College,
Cantho, VietNam

Abstract
Nowadays, due to the expansion of Internet Communication Technology (ICT), people are becoming interconnected via internet environment. Establishing the identity of an individual is highly essential in our network society. The requirement of a reliable user authentication technique is the main concern about networking security, communication and mobility. Biometric technology is a method that is able to recognize a person based on his/her physical or behavioral traits faster and more convenient than the traditional ways such as password and ID cards. This article describes the biometric data acquisition process at an educational institution using a hand vein recognition device in order to authenticate students, workers and professors. Furthermore, it describes the procedure, the device used and some results achieved since the system was implemented.

Keywords
Biometrics, biometric devices, palm vein, security system

1. INTRODUCTION

Biometric technology has been used to recognize people by using biological traits from human being's physiology such as [1],[2]: fingerprint, palm print, vein pattern, hand geometry, iris, face recognition, voice, etc. A biometric system is a pattern recognition system that acquires biometric data from an individual, extracts the features from the acquired data, stores the features as a template and compares them with the template previously stored in the database [3][4].

1.1 Hand vein pattern

Iris and hand vein pattern are unique characteristics in humans and do not change throughout time. The cardiovascular system is the first system formed in the human body. The physical vein arrangement is exclusive for each person. Hand vein pattern is the network of blood vessels located subcutaneously in the hand[5]. Figure 1 shows the vascular network in a hand. Infrared radiation is used to identify vein patterns. Infrared rays penetrate the hand and are absorbed by the hemoglobin present in the blood. The areas where the infrared rays were absorbed are used to create an image pattern which will be digitized and used as a template for identification and authorization [6].

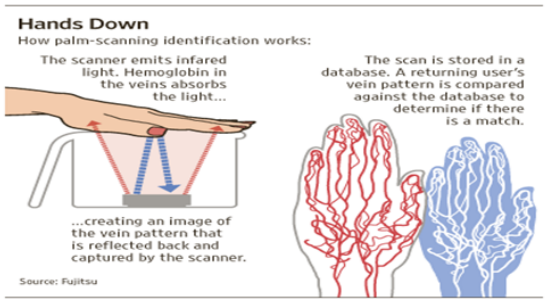

Figure 1: Palm vein authentication [7]

This characteristic is safer than other biometric traits because it does not leave a mark compared with fingerprints and it cannot be easily forged or reproduced like voice. Moreover, it is very difficult to recreate or extract and reuse this characteristic by an impostor. It needs a liveness proof to be authenticated since blood needs to flow into the veins to produce an image, which enhances users' safety[8]. The technology used is noninvasive and contactless which is an advantage where hygienic processes are taken in place [9].

1.2 Advantages

Biometric systems offer various advantages in order to authenticate users in the system [10]. Firstly, users cannot share their biometric characteristics with others as they do with their passwords or smartcards [11]. It is more convenient than passwords/cards because the users don't need to remember, memorize passwords or keep them. Secondly, with the boosting of biometric technology, it creates a new and secure method to make highly accurate verifications of individuals and it cannot be stolen as traditional authentication methods such as: password, card, token, and the like [12]. In fact, attackers cannot counterfeit the user's palm print/iris pattern even using fake or artificial biometric characteristics because most biometric techniques use biological characteristics that cannot be stolen or forgotten. Thirdly, this method can reduce management costs. For instance, with the new

authentication method, the administrators do not need to reissue or issue password/card/token when the users have problems or lose them. Therefore, it can reduce time and cost for management[13]. Palm vein authentication has more advantages than other physical biometric characteristics such as low-resolution imaging, low-intrusiveness, stable line features and low-cost capturing device [12]. Finally, biometric authentication system may be faster than a traditional method, for example: using iris-based, palm vein recognition may take 2 or 3 seconds while finding the smart card or typing the right password, may take 4 or 6 seconds.

1.3 Disadvantages

Biometric technology provides several advantages but it also has some drawbacks such as the cost and cannot be suitable for everyone. Different biometric technology comes along with high deployment costs at the workplace. Some biometric methods cannot be applied to everyone [6], for example: fingerprints are impossible to authenticate someone with no hands; face recognition fails to identify individuals for their whole life because the face changes through time. Furthermore, when biometrics are utilized everywhere in someone's life, all the information is stored in databases; therefore, there is no privacy and can be considered as an intrusive technology.

1.4 Operation

Biometric technique usually uses two basic modes: enrollment and authorization [7]. In the enrollment mode, the characteristics of the user are registered as a sample and stored in a database of the system. Then, in the authorization mode, when using the biometric device, user's characteristics are compared with the stored-template. However, there are two kinds of errors that can happen with a biometric device: False accept (FA) and false rejection (FR). FA can occur when the non-authorized people are authorized as genuine. In contrast, FR happens in rejecting valid people in the system [14].

2. BIOMETRIC TECHNOLOGY IN EDUCATION

Biometric identification market is growing along all the education levels since preschool to universities. According to a 2015 market report by Technavio, in U.S education sector, biometrics market will be expected to reach USD 70 million by 2019. Multifactor authentication and single sign-on features enhance a rapid adoption of this technology. Fingerprints are the most used characteristic followed by vein pattern and voice recognition [15]. Biometric technology has different uses at educational centers. The adoption of this technology is triggered by the necessity of high security levels for protecting students. It is used for granting physical access to the dormitories, canteens or recreational areas also for specific events such as athletic, field trips or dances. At an online level, it is adopted to grant access to digital content and authenticate students during exams by facial recognition through webcams. Another usage is for monitoring the attendance, enrollment and performance of students and teachers. Moreover, it can be used in conjunction with a cashless catering system, where the student is identified by a biometric device and the meal is deducted from a prepaid card [16]. This research describes and analyzes the hand vein identification and authentication process of students, workers and professors at a Hungarian university faculty. Moreover, it highlights some of the results since this process started and provides suggestions and guidelines to improve it, specifically in this education center but also can be relevant in other educational venues.

3. BÁNKI DONÁT FACULTY CASE STUDY

Bánki Donát Faculty of Mechanical and Safety Engineering is part of the Hungarian Óbuda University. As part of the access control system, the faculty implemented a biometric acquisition process in 2013 using fingerprints for identification and granting access to the university's facilities. In 2016 the fingerprint identification was replaced by a more accurate system using palm vein biometric characteristics as the identifier. Its main goal is to protect the faculty facilities and enhance the safety of the university community. The security system also comprises a closed-circuit video surveillance system but for the purpose of this study, just the biometric security technology will be described

3.1 Palm print acquisition procedure

Three palm vein readers were set up at the entrance of the faculty building. They are connected with three turnstiles [figure 2] or the proximity device – tag [figure 3] which allow one person at a time to enter to the building; once the individual presents the palm and the palm reader authenticates the identity. The enrolling step starts at the beginning of the semester. Faculty community users present their palm; the device acquires a template of both hands and stores it. At the beginning of the palm vein acquisition process, the system had a server with the capacity of enrolling 700 users, nowadays this number increased due to the implementation of a new server that can acquire information up to 1500 users. It is possible to create 5 different types of groups according the user's permissions. At the moment there are 3 groups: students, teachers and workers. The biometric data retention time for students is one semester. At the beginning of the following semester all the information is deleted and the students need to enroll again. This procedure prevents students that are not active to get access to the faculty building and updates the database. For workers and professors the information is stored until they are part of the faculty community. The data acquisition process complies with personal data regulation. System users sign a consent which authorizes the faculty to use their biometric traits for identification purposes inside the

faculty premises and gives the opportunity to use an alternative option. Users can choose whether they want to use the palm vein reader device or use a tag that is sold at the faculty, which also functions with the turnstile. The document also states the retention period of the data, which will be deleted at the first day of registration of the following semester. This process complies with purpose and proportionality principles.

Figure 2: Three turnstiles at the entrance gate

Figure 3: The proximity device (Tag)

3.1.1 Users Registered

Figure 4 shows the number of individuals registered in the system since 2013, which was the year the biometric system was implemented at the faculty. In 2014 was the highest number of people registered (7798). The number for 2017 is just the spring semester 2016-2017. It is expected more people registered for the fall semester 2017-2018.

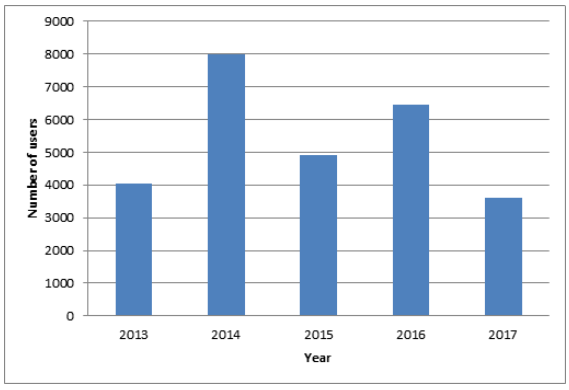

Figure 4: Number of system users per year

3.1.2 Biometric Effectiveness

Figure 5 shows the biometric system effectiveness using the old and the new server compared with the proximity system (tag). The hand vein identification system surpasses the tag system with 14 % using the new server and 10 % with the old server.

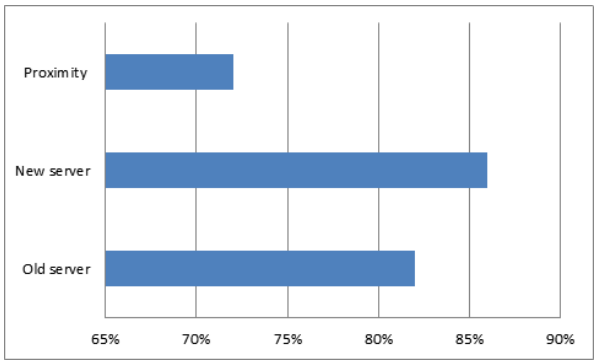

Figure 5: Effectiveness comparison between hand vein identification system and proximity system

3.1.3 The Device

The palm vein reader device has some vital parts such as: palm secure vein sensor, display via LED lights (blue, red, yellow, green) and audio feedback. A sabotage protection is also integrated and it does not require stand-alone power supply because it is provided via USB and CAT cable. The device has the option to be integrated with different systems at an education or industry level. It can be combined with RFID and used with an active directory; therefore, IT administrators can manage only in one surface. . Moreover, this device is a terminal, which is used as a biometric reader in a large or small biometric system, has 256 bit encryption data flow and database. Figure 6 shows a picture of the device and figure 7 shows the actual security system at the faculty

Figure 6: Palm vein reader BS100 [17]

Figure 7: IT administrator in management the system

The requirement for a server which is able to run the palm vein system is not so high. It operates on windows 8

operating system with 16 GB RAM and 1 TB hard drive without connecting to the Internet in order to prevent the security attacks from outside system.

3.2 Functioning

At the enrolling step, the Biosec terminal (BS100) records the individual physical palm veins and uses the data for personal identification. It transfers the signal to BS CONT GK controller. Then the signal continues to send to server via the cables. On the server, the user's characteristics are compared to the stored-template. If they are the same, one signal from the server is sent to the controller again in order to unlock the electric lock gate. In contrast, one signal from the controller is sent to BS100 to turn on the red light to let user try it again because of different reasons such as: overclose distance from user's palm, dirty palm or wrong person. This system [figure 8] also can work in an offline mode, when the connection to the server is interrupted for any reason, the identification process will be taken over by the micro PC which is placed in the controller. Furthermore, one advantage of this system is that it can be integrated via software interface or locally through hardware connection into any other system.

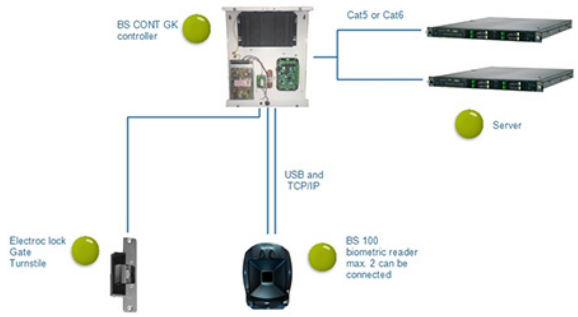

Figure 8: System architecture [17]

4. CONCLUSIONS / RECOMMENDATIONS

The biometric acquisition case study at Bánki Donát faculty is a clear example of how biometric technology is overcoming traditional methods enhancing safety and effectiveness. The biometric system used in Bánki Donát faculty serves its purpose of identify and grant access to the educational facilities for faculty community such as teachers, students and workers. The usage of palm vein authentication system in order to grant access is convenient. It assures that just authorized individuals can use the facilities. The biometric technology adopted at the entrance of Bánki Donát faculty has the potential to be used in other areas such as the library, cafeteria or sporting spaces. Additionally, it can serve for tracking the attendance of students and workers within the faculty. Furthermore, this kind of technology can work more effectively not only in Bánki Donát faculty but also in the other faculties in Óbuda University in specific, and in other Hungarian universities in general.

1. 5. REFERENCES

1 [1] A. Ross, "Human recognition using biometrics: an overview," Ann. Des Telecommun., vol. 62, no. 1, pp. 11–35, 2007.
2 [2] M. W. David Zhang, Guang-Ming Lu, Adams Wai-Kin Kong, "Online Palmprint Indentification system for civil applications," Comput. Sci. Technol., vol. 20, no. 1, pp. 70–76.
3 [3] "Vascular network in hand." .
4 [4] I. Biometrics, No Title. .
5 [5] S. Crisan, "Biometric Security and Privacy," pp. 21–50, 2017.
6 [6] a. Nadort, "The hand vein pattern used as a biometric feature," Master Lit. Thesis, no. May, p. 162, 2007.
7 [7] M. Watanabe, "Palm vein authentication," Advances in Biometrics: Sensors, Algorithms and Systems, 2008. .
8 [8] K. Yang, E. Y. Du, and Z. Zhou, "Consent biometrics," Neurocomputing, vol. 100, pp. 153–162, 2013.
9 [9] "Vascular Pattern Recognition," 2012. .
10 [10] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," IEEE Secur. Priv. Mag., vol. 1, no. 2, pp. 33–42, 2003.
11 [11] H. P. D. Nguyen, "Fingerprint Device (Suprema) Is Safe or Not ?," Hadmérnök, vol. 4, pp. 10–18, 2016.
12 [12] M. G. K. Ong, C. Tee, and A. T. B. Jin, "Touch-less palm print biometric system," Visapp 2008 Proc. Third Int. Conf. Comput. Vis. Theory Appl. Vol 2, pp. 423–430, 2008.
13 [13] Growth Business Co, "Biometrics in Business," Growth Business UK, 2005. [Online]. Available: http://www.growthbusiness.co.uk/biometrics-in-business-18454/.
14 [14] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan, "Reference Threshold Calculation for Biometric Authentication," Int. J. Image, Graph. Signal Process., vol. 6, no. January, pp. 46–53, 2014.
15 [15] "Technavio, "Biometrics Market in the United States in Education Sector 2015-2019."
16 [16] "I. Inc, "Biometrics in Education- A Growing Demand." .
17 [17] "Palm system architecture." .
18