Journal of Mobile, Embedded and Distributed Systems, vol. VII, no. 1, 2015
ISSN 2067 – 4074

Biometric Security - Fingerprint Recognition System

Alexandra–Emanuela VĂCĂRUȘ
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
alexvacarus@gmail.com

Abstract: The paper presents an application, FingerTouch that provides a secure method of storing usernames and passwords for different types of accounts by using biometric fingerprint authentication. Recent developments in the smartphone area regarding fingerprint authentication on mobile devices is discussed. The purpose of the application and the technologies that were used in the development are described. The features, architecture and implementation of the application are analyzed.

Key-Words: Fingerprint, Authentication, Password, User, Administrator, Mail, Social, Media

1. Introduction – Fingerprint Biometrics

Biometrics represent the perfect solution to the problem of digital authentication, by measuring unique physical characteristics. Compared to other, more traditional token-based approaches, biometric authentication of a person is quick, reliable, efficient, safe, secure and easy to use method.
Fingerprint identification has been an effective way of replacing passwords, because it gives a higher level of security.
One of the main differences between systems that use passwords for authentication and those that use biometric methods is that password systems don't have an identity. The security of a password cannot be guaranteed because it can be guessed, stolen or given to other users and so we can never be perfectly sure that the person that tries to gain access is the actual owner of that password.
Although, the range of available fingerprint scanners varies a lot, the principle on which they function and the way that a person is identified is mostly the same. An image of the tip of the finger is taken with a light-sensitive device like a scanner, then it is pre-processed and the features are extracted. After it is brought in digital format, the image is compared to the templates that were created when the enrolment took place.

In order to set up a biometric system the most important step is the enrolment. Depending on the device that is being used, the enrolment procedures differ, but generally require scanning the necessary biometric data a few times to obtain an accurate measurement. The more correct the enrollment is, the more accurate the authentication will be. So it is very important that the finger is in an appropriate position and enough pressure is applied when acquiring the fingerprints so that no false readings appear.
FAR – False acceptance rate is the probability that a user's fingerprint will be matched with a different user's enrolment template. The goal for most biometric systems is to maintain the FAR as low as possible, so that an imposter cannot access the system as a legitimate user.

$$FAR = \frac{NFA}{NAR} \qquad (1)$$

$$where\ NFA = Number\ of\ false\ acceptance$$
$$NAR = number\ of\ authentication\ requests$$

FRR – False rejection rate is the probability that a user's fingerprint is not recognized as matching the template that was acquired during enrolment. A high value of FRR can cause a legitimate user to be rejected and denied access to the resources.

$$FRR = \frac{NFR}{NAR} \qquad (2)$$

where:

$$NFA = Number\ of\ false\ rejects$$
$$NAR = number\ of\ authentication\ requests$$

2. Fingerprint authentication on smartphones

Today, smartphones have new fingerprint scanning features that facilitate authentication and online transactions.
The applications for fingerprint authentication are mainly used to replace passwords, personal identification numbers and patterns for unlocking a gadget.
In 2013 Apple included a fingerprint scanner in the iPhone 5S is currently working on a concept called EasyPay, which represents a mobile payment solution.
Samsung included a fingerprint scanner in its latest phone, the Galaxy S5. An SDK for the Galaxy S5 is also available, so that developers can incorporate it into their software.
At the 2014 Mobile World Congress, Samsung and PayPal announced a collaboration through which PayPal will be the first global payments company to support Samsung Galaxy S5's mobile fingerprint authentication technology.
The biometric systems on both smartphones were hacked by german researchers (CCC – Chaos Computer Club and SRLabs – Security Research Labs) a few days after the official release of the devices.

3. Application purpose

The FingerTouch application comes as a solution to the existing problem of password loss or forgetfulness. According to a study conducted by Abbas Moallem of the San Jose State University [23]
„People have a tendency to use a very small number of passwords, and
they often keep track of those passwords most likely in paper format since a very
strong percentage of people respond that they rarely use passport retrieval, especially
among the older age group. Users know answers to the security questions of several
people around them, and they might be able to answer them and get access to the password if they can get control of the email box.”.

Taking into consideration the large number of applications that require a username and a password, the fact that people should try to diversify this fragile information and the effort that they make to remember it, the existence of the FingerTouch application is justified. It meets the needs of PC users to remember and to store their usernames and passwords to various accounts, in a safe and secure way.

4. Technologies used

The application was developed using the Java programming language (i.e. Java 7) and the Netbeans v7.2 IDE. For data storage, the application communicates with a Firebird database. Firebird was chosen because it is a stable, easy to install, low maintenance database which can be stored at any location and easily moved.
The biometric fingerprint reader used is a Futronic FS84 ethernet interfaced reader.It has an internal 64Kb RAM memory in which it stores information regarding enrolled fingerprints (user id, finger id, group id, user type: ordinary, VIP, and the fingerprint itself in the form of byte string.

5. Application features

After launching the application, the user needs to authenticate himself / herself, in order to gain access to the available features. The authentication button "Autentificare" opens the login frame. After clicking the "Ok" button from this window, the reader enters its identification module and waits for the user's finger to touch the screen. If the identification is successful, the user is logged into the application, otherwise, an error message stating the fact that the user was unknown is shown on the screen.

ISSN 2067 – 4074

FingerTouch provides the possibility of registering two types of users: ordinary users and administrators. The users have a restricted access to certain parts of the application that the administrators (or users with full rights) have. What users with administrator rights can do in addition is to enroll and add new application users, to identify and verify them and also to delete them. Figure 1 shows the application in the middle of the login procedure, when the reader waits for the fingerprint of the user.

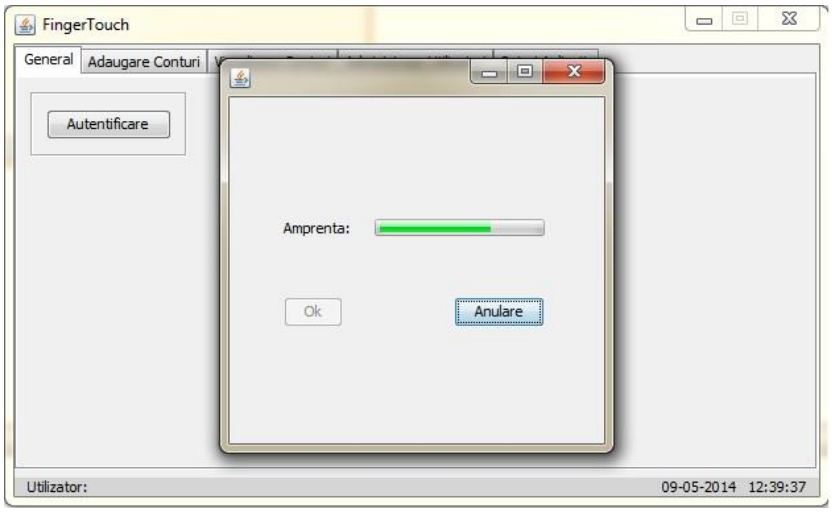

Figure 1. Login frame with the authentification in progress

The registration of a new user for the application is done first by accessing the tab for users management - „Administrare utilizatori". This window consists of a table representing all the users that are enrolled and have access to the application, as well as a group of buttons that define certain user manipulation functions like: enrolling a new user, deleting an existing one, identifying and verifying users.
The „Inregistrare" button opens the enrollment frame. Here, the administrator has to fill in all the necessary data like last name, first name, telephone number, personal numeric code etc., then a username and password is assigned to each user along with the access rights (limited or total). When the „Start" button is pressed, the reader enters the enrollment module in which it waits for the user to touch the screen. For the purpose of this application the reader aquires three samples of the same fingerprint.
Figure 2 shows the enrollment step in progress with the personal data of the user already submitted and the reader waiting for another sample of the fingerprint.

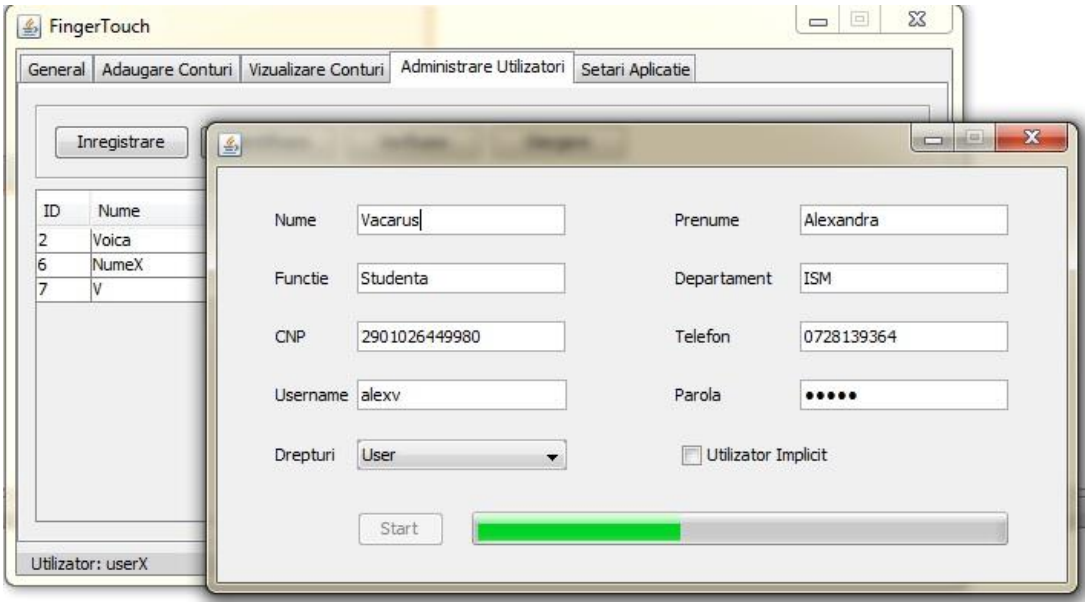

Figure 2. Enrollment process with the reader waiting for a fingerprint sample

After the enrollment, the user has been granted the right to login and use the application. The features that the users can access are found in the "Adaugare Conturi" (add accounts) and "Vizualizare Conturi" (view accounts) tabs. The user can add accounts belonging to three bigger categories: mail accounts, social media accounts and communication accounts. The featured mail accounts are Yahoo, Gmail and Hotmail. The social media accounts can be: Facebook, Twitter and Instagram accounts, and for the communication accounts Skype was chosen. When choosing a certain account category and an account type the user has the possibility to give a name to that account (i.e. Facebook1, Facebook2, for he/she may have more than one account for a certain application). Then the the username and password for accesing that account are provided and by clicking the save button "Salvare" the information regarding this account is saved. By following the same procedure, the user can add any number of accounts and store all their corresponding usernames and passwords.

When the user is done adding accounts, he can simply view them by accessing the view accounts tab "Vizualizare Conturi". From here all he has to do is chose a category, a type of account and then on the right side of the window a he will see a combo box populated with all the accounts that match the selection. From that combo box he can choose the desired account and visualize its username and password. Also from this window, the user has the possibility to edit the information for a certain account and also to delete an account.

Figure 3 shows the tab for account viewing – "Vizualizare Conturi" with a selected Twitter account and its respective username and password information in the text fields.

ISSN 2067 – 4074

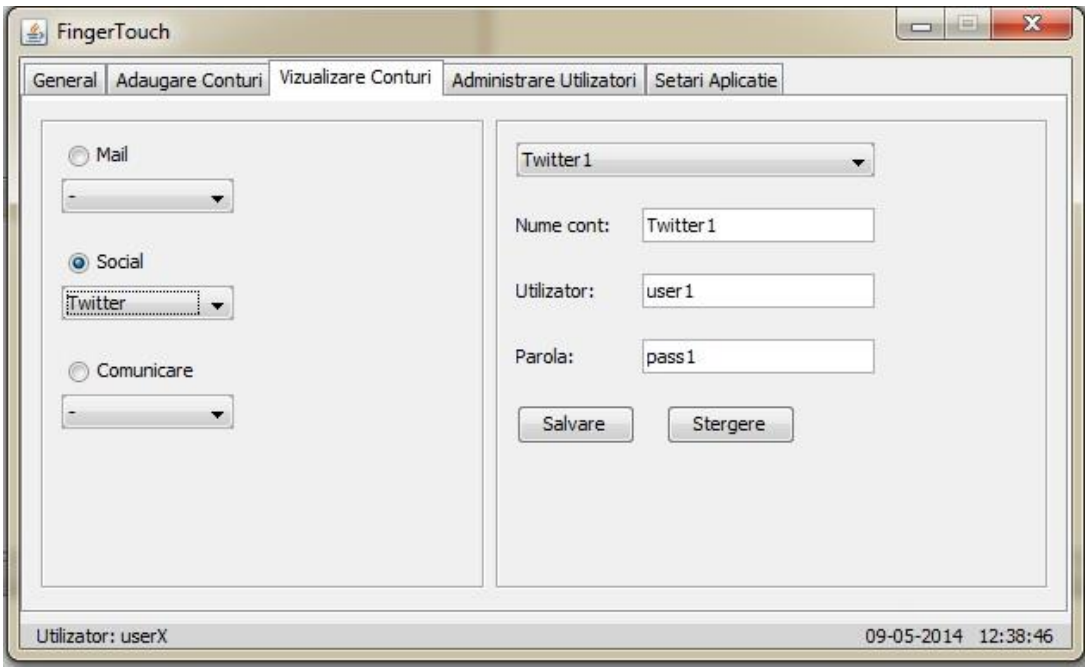

Figure 3. The „Vizualizare Conturi" tab showing account information for a Twitter account

6. Architecture

Regarding the architecture of the application, there are several aspects that should be considered. The application is developed in Java, using the Netbeans Ide. It communicates with a Firebird database which stores information regarding users (the data fields required during enrollment, to which the extracted fingerprint from the reader is added), information about application activities in the form of logs and a one final table containing hash values (whose functionality will be discussed shortly). The application uses an external file in which it stores the application usernames and password given at enrollment. This data is encrypted in the file so it can't be viewed by anyone who tries to open and read its contents. This file was used a security measure, to avoid storing sensitive information like usernames and passwords in the database. When a user is registered for the first time into the application, a personal folder is created at a specific location on the disk. The name of that folder is also encrypted so if accessed, the folder name cannot give any information regarding its contents. In this personal folder, the application will store, in the form of encrypted files, the data for the media accounts that the user will add. All these folders and files, when accessed, give absolutely no clear information regarding their contents. If a user tries to guess which folder or file is his, he would still not be able to decipher the data within them. The only way he can do that is by logging into the FingerTouch application and selecting the tab for viewing accounts, then he will get all the information he needs.

Figure 4 shows a scheme representing the architecture of the application with the components described earlier.

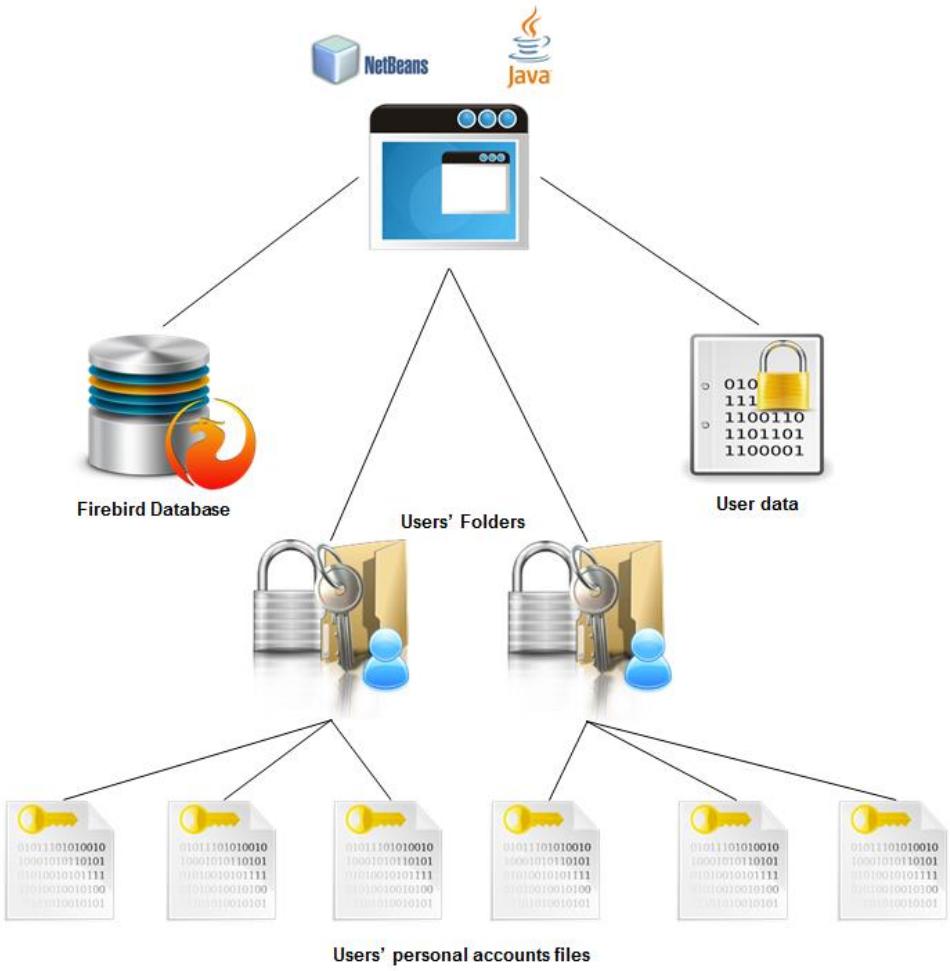

Figure 4. FingerTouch architecture

7. Additional security measures in implementation

When it came to implementing the database connection, it was important not to store the username and password for the database user in clear text in the code of the application. The table in the database containing hash values, which was mentioned earlier serves as a security check for the file in which the application user passwords and usernames are stored. It works in the following manner: when a new user is registered and its username and password are stored in the encrypted file on the disk, a hash of this file is created and sent to the database. When the application starts, it compares the last hash from the database with the one computed by applying a new hash on the encrypted file on the disk. If the hash values are identical then the file is ok. This helps to notify the user in case that someone tries to change, or alter the contents of the encrypted file with malicious intentions.

8. Conclusion

The "Finger touch" application, developed in Java, gives the opportunity to create, store and manage in a very secure way identification data (usernames and passwords) for e-mail, social media and communication with a user account and also as an administrator account. The administrator is able to manage the application users in a very efficient way due to the application accessibility.

Acknowledgement

Parts of this paper were presented at The 7th International Conference on Security for

ISSN 2067 – 4074

Information Technology and Communications (SECITC 2014), Bucharest, Romania, 12-13 June 2014.

References

[1] A.H. Aboalsamh, „Vein and fingerprint biometric authentication: future trends", in *International journal of computers and communication*, issue 4, vol. 3, 2009.

[2] J. Ashbourn, „Practical Biometrics – From aspiration to Implementation", Springer Velag, 2004.

[3] R. Aufreiter, „Der Finger als Schlussel – Aktuelle Biometrieverfahren im praktischen Einsatz", Utimaco Safeware AG, 2003.

[4] R. Bansal, P. Sehgal, P. Bedi, „Minutiae Extraction from fingerprint images – a review", in *IJCSI International Journal of Computer Science Issues*, 2011.

[5] B. Bhanu, X. Tan, „Computational Algorithms for Fingerprint Recognition", Kluwer Academic Publishers, USA, 2004.

[6] R. M. Bolle, J. H. Connell, S. Pankati, N. K. Ratha, A.W. Senior, „Guide to Biometrics", Springer Verlag, 2004.

[7] J. Chirillo, S. Blaul, „Implementing Biometric Security", Wiley Publishing, 2003.

[8] Digital Persona – DigitalPersona White Paper, *Guide to fingerprint recognition",* Available: http://www.itworksolutions.com/brochure/catalogue/digitalpersona/Fingerprint%20Guide.pdf

[9] J. Feng, A. K. Jain, K. Nandakumar, „Biometrics: Fingerprint Matching", IEEE Computer Society, 2010.

[10] „Fingerprint Verification Competition 2006", Available: http://bias.csr.unibo.it/fvc2006.

[11] P. Gregory, M. A. Simon, „Biometrics for dummies", Wiley Publishing Inc, 2008.

[12] Griaule Biometrics, Available: http://www.griaulebiometrics.com/page/en-us/fingerprint_sdk.

[13] A. K. Jain, A. Ross, S. Prabhakar, „Fingerprint matching using minutiae and texture features", in ICIP, 2001.

[14] A. K. Jain, Z. Li, „Encyclopedia of Biometrics", Springer 2009.

[15] K. Karu, A. K. Jain, „Fingerprint classification", in *Pattern Recognition*, vol. 29, no. 3, pp. 389-404, 1996.

[16] D. A. Katz, „Fingerprinting", 2005.

[17] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, „Handbook of Fingerprint Recognition", Springer, 2003.

[18] D. Maltoni, „A Tutorial on Fingerprint Recognition", Biometric Systems Laboratory - DEIS - University of Bologna, 2005.

[19] Neurotechnology, „VeriFinger SDK", Available: http://www.neurotechnology.com/verifinger.html.

[20] C. Roberts, „Biometric Technologies, Fingerprints", 2006.

[21] A. Ross, A. K. Jain, J. Reisman, „A hybrid fingerprint matcher" in *Pattern Recognition*, vol. 36, 2003.

[22] A. Ross, J. Reisman, A. K. Jain, „Fingerprint matching using feature space correlation" in *Proc. of Post-ECCV Workshop on Biometric Authentication*, LNCS 2359, pp.48-57, Denmark, June 1, 2002.

[23] A. Moallem, "Did you forget your password?", Available: http://www.engr.sjsu.edu/amoallem/publications/HCII2011_didYou_67700029.pdf