Series: ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE – ECAI-2015

Contents

Vol. 7 – No. 1/ 2015 ISSN – 1843 – 2115

Media	IEEE Catalog Number	ISBN
Compliant PDF Files	CFP1527U-ART	978-1-4673-6647-2
DVD	CFP1527U-DVD	978-1-4673-6645-8
Print	CFP1527U-PRT	978-1-4673-6646-5

UNIVERSITY OF PITESTI

&

LUMINA – THE UNIVERSITY OF SOUTH EAST EUROPE

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII ŞTIINŢIFICE

UNIVERSITATEA EUROPEI DE SUD-EST LUMINA

Technical sponsorship

IEEE Romania section

IEEE Industry Applications Society

Proceedings of the International Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE – ECAI-2015

ELECTRONICS COMPUTERS AND ARTIFICIAL INTELLIGENCE

Series: ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE

Vol. 7 – No. 1/ 2015 ISSN – 1843 – 2115

Media	IEEE Catalog Number	ISBN
Compliant PDF Files	CFP1527U-ART	978-1-4673-6647-2
DVD	CFP1527U-DVD	978-1-4673-6645-8
Print	CFP1527U-PRT	978-1-4673-6646-5

Series: ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE – ECAI-2015

Contents

Vol. 7 – No. 1/ 2015 ISSN – 1843 – 2115

Media	IEEE Catalog Number	ISBN
Compliant PDF Files	CFP1527U-ART	978-1-4673-6647-2
DVD	CFP1527U-DVD	978-1-4673-6645-8
Print	CFP1527U-PRT	978-1-4673-6646-5

ECAI-2015 ORGANIZERS

UNIVERSITY OF PITESTI
Faculty of Electronics, Communications and Computers

UNIVERSITY OF S-E EUROPE 'LUMINA',BUCHAREST
Faculty of Engineering: Department of Information Technology and Communication

POLITEHNICA UNIVERSITY OF BUCHAREST
Faculty of Electronics, Telecommunications and Information Technology
Faculty of Automatic Control and Computers

MILITARY TECHNICAL ACADEMY, BUCHAREST
Faculty of Electronics and Informatics Military Systems

FUZZY LOGIC SYSTEMS INSTITUTE, FUKUOKA, JAPAN

NEVŞEHİR HACI BEKTAŞ VELİ UNİVERSİTY
Faculty of Engineering and Architecture
Nevşehir Vocational School

PETROLEUM - GAS UNIVERSITY OF PLOIESTI
Department of Automation, Computers and Electronics

NATIONAL COMMUNICATIONS STUDIES AND RESEARCH INSTITUTE INSCC- Bucharest

NUCLEAR RESEARCH INSTITUTE
Mioveni

'GHEORGHE ASACHI' TECHNICAL UNIVERSITY, IASI
Faculty of Electronics, Telecommunications and Information Technology

'VALAHIA' UNIVERSITY, TARGOVISTE
Faculty of Electrical Engineering, Electronics and Information Technology

INSTITUTE OF COMPUTER SCIENCE OF THE ROMANIAN ACADEMY
Iasi Branch

Edited by University of PITESTI
ADDRESS: Street Târgu din Vale, No. 1, 110040, Piteşti, Argeş Romania
978-1-4673-6647-2/15/$31.00 ©2015 IEEE

ECAI 2015 - International Conference – 7th Edition
Electronics, Computers and Artificial Intelligence
25 June -27 June, 2015, Bucharest, ROMÂNIA

Fingerprints used for security enhancement of online banking authentication process

Cătălin LUPU, Vasile-Gheorghiţă GĂITAN
Faculty of Electrical Engineering and Computer Science "Ştefan cel Mare" University
Suceava, Romania
catalinlupu@seap.usv.ro, gaitan@eed.usv.ro

Valeriu LUPU
Faculty of Economics and Public Administration
"Ştefan cel Mare" University
Suceava, Romania
valeriul@seap.usv.ro

***Abstract* – Online banking services have become one of the most important applications on the Internet, being provided by most of the banks all over the world. The end-user can manage the accounts or make some payments without being forced to go to the physical bank office. That's why security concerns regarding authentication have to be taken into the account and the bank should provide various and combined methods for login, in order to increase the confidence in their services. In other words, the bank should provide a multi-factor authentication. This paper will present a model for user enrollment and authentication, using three basic methods, based on: what user knows (a username), what user has (a digipass) and an intrinsic characteristic of the user, e.g. a fingerprint. Combining these three characteristics will lead to a great security improvement in authentication or order signing. Classical methods are based only on the first two characteristics (what user knows and has), without the most habitual one, that cannot be lost or stolen: an intrinsic characteristic of the user, like a fingerprint or an iris. This paper will also present an application developed during our researches, for user enrollment that can be used in the bank-side environment.**

Keywords- online banking; security; biometrics; enrollment; process flowchart

I. INTRODUCTION

Online banking services have been in use since the beginnings of the 1980's and are still in a continuous development. Most of the banks are providing this kind of services to their clients in order to reduce the classic transactions and to facilitate the user's operations. For example, someone receives the salary in a bank account, and using internet banking can make payments or see an overview on the available resources, without going to a bank office. Actually, using internet banking, the user does not have even to know where the bank office is, excepting some specific cases: when there are not anymore money into the account and the user has to deposit some cash into the accounts, when a credit card expires or when a digipass isn't working anymore. Almost all payments can be done by using internet banking or credit cards, so the user doesn't have any reason to go to the physical bank office, while "virtual" (or online, e-) banking service provides almost the same facilities.

Security in online banking authentication can vary from the classic username and static password-based method to more advanced techniques that uses an username and a dynamically generated password (also called OTP – "One Time Password"), through a physical or a virtual digipass. These methods are based on what user knows/remembers (a username, a password) or have (a virtual or physical digipass). But the main problem is that these things can be forgotten, lost or stolen. That's why using what user is (a specific, particular characteristic that uniquely identifies an individual, like fingerprints, iris, voice, face, etc.) in online banking authentication will lead to a great security improvement. A combination of these three (what user knows/has/is) will also lead to a better security than using only two of them.

In the following paragraph we will present the state of the art in online-banking authentication using biometrics.

II. STATE OF THE ART

The idea of using biometric characteristics for online banking authentication isn't a new one but there are only a few implementations of this concept, especially for testing purposes. Also, only a few researches have been done in this field, for example by searching IEEE Xplore with the terms "fingerprint online banking" will lead to only 14 results, "biometrics online banking" displays only 27 results and "biometrics security banking" shows 116 papers, from the total number of almost 4.000.000 indexed items. For the last searched phrase, most of the articles appeared after the 2000's, with only 6 older articles that this time span. That's why we can consider that many rigorous researches have to be done in this field.

A very interesting paper ([1]) was published in 2012, where the authors are describing their researches in using biometrics for various forms of banking: ATMs (1st place - 45% from 121 studied banks), access control to the bank's computers (2nd place – 24%), branch-banking (3rd place, almost equal to access control – 22%), internet banking (4th place – only 10%), POS devices (with only 2%) or telephone banking for password/PIN reset. We can also see that Asia is in the front of using biometrics in banking, with a percent of 52%, followed by America (32%) and Europe (9%). As biometric characteristic, the fingerprints are on the first place (48%), followed by finger vein, voice, hand vein, iris (7.43%) and

signature. Other biometrics are under 5% in their researches.

Other representative papers in this field are represented by [2] and [3], the authors describing their researches in biometrics used for ATMs.

During our researches, we published papers in the domain of this paper, more relevant being [4] and [5]. In the papers [6] and [7] we presented the beginnings of using fingerprints for personal recognition and the design of an optimal filter for fingerprint's image enhancement and restoration.

Some banks are using fingerprints for authentication, for example United Bankers' Bank (with the webpage for login available at reference [8]). This bank is using the U.are.U sensor for fingerprint acquiring and the Digital Persona Online Client 4.4.1 software as the interface between the sensor and the webpage. However, this webpage has some limitations, because it is browser-dependent (only Internet Explorer is accepted, with a version greater than 8.0, as it can be seen on the reference [9]) and needs additional software to be installed: Silverlight and Microsoft .NET Framework with a version greater than 4.0. For example, by accessing this page on a Windows 7 x64 from Internet Explorer 11.0, the result will be that the browser is not acceptable, being identified as "Internet Explorer 9.0" (notice that there is no blank space between "Internet" and "Explorer"). Also, this webpage is also sensor-dependent, because it only works with U.are.U sensors. Hence, we can conclude that this application is intended to be accessed only from a desktop or a notebook computer that is equipped with a U.are.U fingerprint sensor, and it is not suitable to be accessed from a mobile device like a smart phone, a PDA or a tablet device.

The main purpose is to design an application that can be accessed from any device, using the same level of security on all of them.

Next, we will present a model that is intended to be used for online banking applications, both from end-user side and bank-side medium.

III. Proposed Model for Online Banking Application

The online banking application model can be seen from two points of view: end-user interface and bank officer application for account management. In the following paragraphs both of these two sides of the application will be described. Figure 1 presents an overview on what we will discuss further.

A. End-user interface

When the user accesses the online banking, an authentication page is delivered through a secure channel, using SSL or TLS as cryptographic protocols. For stronger security, the user has to use all these three methods: what *knows* (username and PIN for digipass), what *has* (a digipass) and what *is* (a fingerprint previously registered in the bank's database). After successful logon, the user can make some operations on the account, like seeing an overview on available resources, loans or to make payments (paying bills or transfer funds to other accounts). The digipass and registered fingerprint should also be used for online operations signing. An order is at this moment signed using a digipass code or the login password. But fingerprints should also be used to increase the transaction security. On his account, the user can also constitute or clears the deposits or to make other actions, like seeing account statements or credit card status.

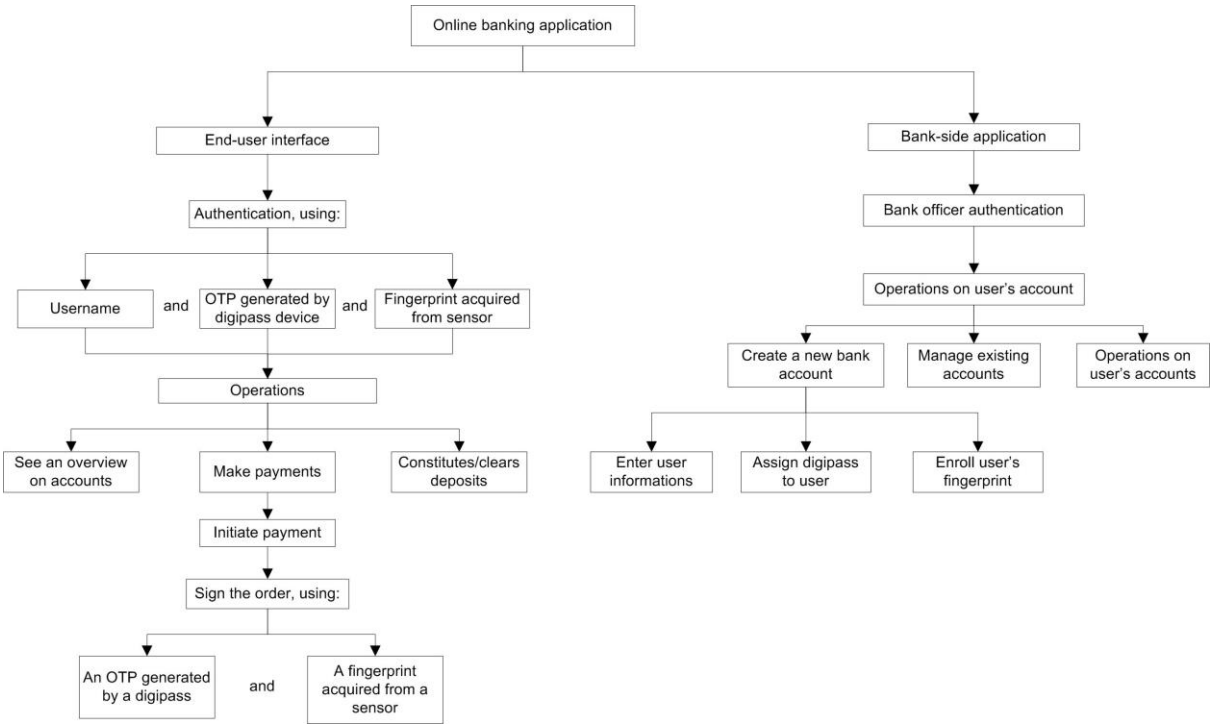

Figure 1. Online banking application overview

B. Bank-side application

In the bank-side environment, the bank officer, after successful authentication, can make some operations on user's account(s). A new account can be created or existing accounts can be managed or closed. Also, operations (like transactions, deposits, etc.) can be made on the user's account.

When creating a new account, the bank officer has to introduce the user's details and then to assign him/her a unique bank account. Next, a digipass has to be assigned to the user, being linked with the bank account. The user will be asked to change the default digipass password to an easier to remember one. After these steps, the user has to provide a fingerprint in order to be registered in the bank's database. After all went well, the user can use the online banking application in order to authenticate using all of the provided credentials. If the user doesn't possess a fingerprint scanner, then it will be provided by the bank.

In the next paragraph we will present an application developed for user enrollment.

IV. APPLICATION FOR USER ENROLLMENT

During our researches, we developed a VB.NET application for initial or further enrollment of a user in an online banking application. We chose Microsoft Fingerprint Scanner for fingerprint acquirement. The sensor is presented in figure 2. This fingerprint sensor is an optical one, providing high-resolution images. The sensor comes with software for fingerprint enrollment and identification, created by Digital Persona, called "Password Manager". This device is really inexpensive and provides good fingerprint images that can be processed in order to enroll, identify or verify a person.

Figure 2. Microsoft Fingerprint Sensor

We focused on the development of an application for user enrollment (bank-side software), the authentication part (client-side) being in a developing process. The main form of this application is presented in the figure 3. We used the sensor described above, together with GrFinger library from Griaule Biometric's Fingerprint SDK 2009 ([10]). We used the Griaule FingerCap USB driver 2.1, provided by the same company, because the original sensor's software doesn't have a SDK that can be used for application development.

From the GrFinger library, we used only the functions for initializing fingerprint sensor and for acquiring RAW fingerprint images. For image enhancement we used the algorithm proposed in the paper [7] and for feature extraction, template creation and matching the methods described in the book [11] were used.

The main idea is that five impressions of the same fingerprint are taken, each acquired image being compared with the ones already introduced. When capturing the fingerprint we decide if it is suitable for personal recognition or not. If the fingerprint is denied, then the user has to repeat the current attempt until an acceptable fingerprint is acquired. After the second fingerprint, all further images are compared against the already acquired images, and if the match score is above a threshold established into the software, then the password is accepted, otherwise it is rejected and the user has to reintroduce it.

After all fingerprints have been acquired, in compliance with the conditions described above, the enrollment process finishes and the user can use his credentials in order to login to the internet banking application. The final page, after successful enrollment is presented in the figure 4.

This software can be used both for initial enrollment or further registration, in the following cases: (i) the user has only a username and a password and needs a fingerprint to be registered for security enhancement; (ii) because of a physical impairment that occurs after initial enrollment, the user can provide another fingerprint than the one registered in the system.

V. CONCLUSIONS AND FUTURE RESEARCHES

The main problem with actual authentication methods is that are using only credentials that can be stolen or lost. Using a characteristic that a user always possesses (like a fingerprint), together with actual methods, will lead to a security enhancement, being suitable even for the most suspicious and reticent users. The main target in future research is to develop an application that is sensor-independent and that can be used on various devices, not only on desktop or notebook computers. Also, the designed application must be operating system-independent, being suitable to be used on Linux, Android, iOS or others, not only on Microsoft Windows environment. Many researches can be done in raising the security level, especially regarding template transfer to the bank's server or predicting spoofing attack that can occur in using fingerprints. Many biometrics can be taken into account, like iris or face recognition, but keeping the implementation price as low as possible (for example a basic iris scanner costs around $100, while the fingerprint sensor presented above is as low as $30). Of course, when we talk about the prices, we refer to the bank's costs, as the devices should be provided freely to the end-users.

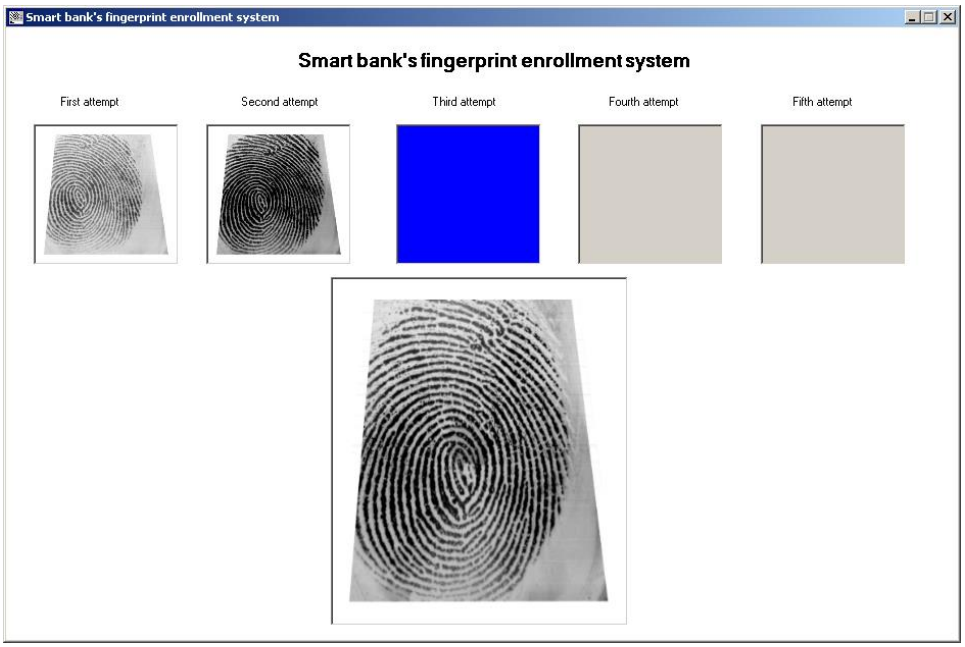

Figure 3. Application for fingerprint enrollment

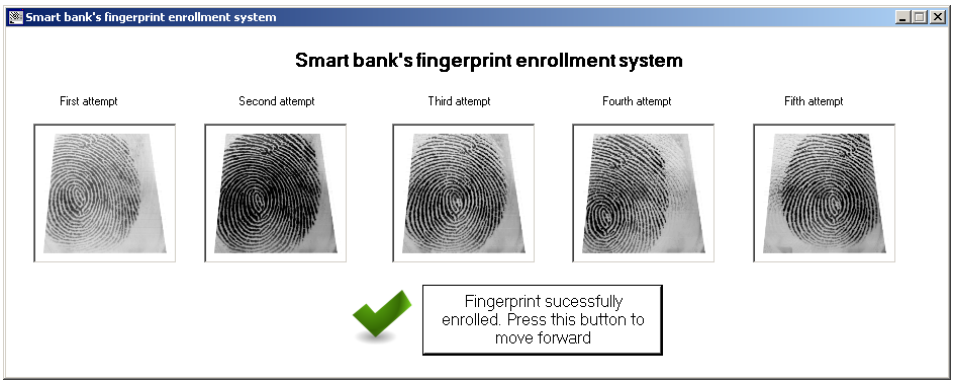

Figure 4. Successful enrollment message

ACKNOWLEDGMENT

This paper was supported by the project "Sustainable performance in doctoral and post-doctoral research PERFORM - Contract no. POSDRU/159/1.5/S/138963", project co-funded from European Social Fund through Sectorial Operational Program Human Resources 2007-2013.

REFERENCES

[1] S.S. Hoseini and S. Mohammadi, *"Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system"*, Journal of Basic and Applied Scientific Research, Part III 2(9), September 2012, pp. 9152-9160

[2] A. Abayomi-Alli, E.O. Omidiora, S.O. Olabiyisi, J.A. Ojo, *"Enhanced e-banking system with match-on-card fingerprint authentication and multi-account ATM card"*, The Journal of Computer Science and its applications, Vol. 19, No. 2, Dec. 2012, pp. 14-22, ISSN 2006-5523

[3] M.O. Onyesolu, A.O. Akanwa, O. McChester, V.C. Nwasor, "*Robust Authentication Model for ATM: a Biometric Strategy Measure for Enhancing E-Banking Security in Nigeria"*, International Journal of Advanced Research in Computer Science, Volume 3, No. 5, Sep-Oct 2012, pp. 164-169, ISSN 0976-5697

[4] C., Lupu, V.G., Găitan, V. Lupu, *"Security enhancement of internet banking applications by using multimodal biometrics"*, IEEE 13th International Symposyum on Applied Machine Intelligence and Informatics (SAMI 2015), Slovakia, pp. 47-52, ISBN 978-1-4799-8220-2, 978-1-4799-8221-9,

[5] C. Lupu, V. Lupu, *"Biometrics used for authentication in internet-banking applications"*, Annals of the „Constantin Brancusi" University of Targu Jiu, Engineering Series, No. 3/2014, pp. 57-63, ISSN 1842-4856

[6] C. Lupu, V. Lupu, *"The beginnings of using fingerprints as biometric characteristics for personal identfication purposes"*, Annals of the „Constantin Brancusi" University of Targu Jiu, Engineering Series, No. 3/2014, pp. 53-56, ISSN 1842-4856

[7] C. Lupu, "*Development of optimal filters obtained through convolution methods, used for fingerprint image enhancement and restoration*", "The USV annals of Economics and Public Administration", Volume 14, issue 2(20), 2014, pp. 156-167, ISSN 2285–3332 (printed), 2344–3847 (online)

[8] United Bankers' Bank login page, available at: https://sso.unet.ubb.com/Login/Login.aspx (last accessed on Feb. 15, 2015)

[9] United Bankers' Bank minimum requirements check web page, available at https://sso.unet.ubb.com/troubleshooting/requirements.aspx (last accessed on May 15, 2015)

[10] Griaule Biometric's Fingerprint SDK 2009, available at http://www.griaulebiometrics.com/page/en-us/downloads (last accessed on Feb. 15, 2015)

[11] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "*Handbook of fingerprint recognition*", Springer,2005, ISBN 0-387-95431-7