Fingerprint Verification as a Service in KC CLASS

Jernej Bule, Peter Peer
Faculty of Computer and Information Science, University of Ljubljana,
Tržaška cesta 25, 1000 Ljubljana, Slovenia
E-mail: {jernej.bule, peter.peer}@fri.uni-lj.si

Abstract - The aim of our work is the implementation of biometric verification based on fingerprints in a cloud platform. Within this work we: 1) develop our own system for verification of persons based on fingerprints, 2) integrate system in a cloud platform, 3) address aspect of data security and authentication data fusion, 4) use modified e-learning system as a test environment for proof-of-concept. A pilot version of the entire system is already installed.

I. INTRODUCTION

When we talk about Internet authentication, for the vast majority, we are still talking about passwords. The biggest problem with current authentication approaches is too many password-account pairings for each person to remember, which leads to forgetting or using the same username and password for multiple sites [1]. Some people see a solution in the use of biometrics. Biometrics methods are already quite widely used for local authentication (in private use), while authentication on the Internet using biometrics is still relatively unused. There are problems that need to be solved, before biometric services can be applied massively. More widespread use is mainly limited by law. In Slovenia we have strong legislation in this area, which allows use of biometrics only in exceptional cases, where specific information cannot be protected adequately [9]. In other countries, especially in the USA, biometric services are used more, because the law is less restrictive.

In the last few years the number of biometric data extremely increased. For example, over the next few years, biometrics databases for Federal Bureau of Investigations, Department of State, Department of Defense, and the Department of Homeland Security are expected to grow to accommodate hundreds of millions, if not billions of identities [2].

The quantity of information to be stored gets even larger when you consider that several biometric modalities are associated with each identity in these

databases. These are typically fingerprints, but there are also facial and iris images, voice patterns, palm print patterns etc. Local solutions cannot meet these requirements, it is necessary to find alternative solutions. Cloud computing represents a solution with its almost unlimited storage capacity and capability of rapid data distribution and parallel processing.

In this article, we introduce our own system for verification based on fingerprints and show concept of its integration in a cloud platform.

II. FINGERPRINT VERIFICATION IN THE CLOUD

A. Fingerprint verification system

Through participation in the KC CLASS [6] we develop our own system for verification based on fingerprints called FingerIdent [3]. Test version already operates at the Faculty of Computer and Information Science, in front of the Computer Vision Laboratory.

General functions of FingerIdent can be divided into two main parts (Figure 1). These are: user registration (enrollment) and the verification process.

The registration process is using fingerprint reader to capture the data. The next phase is to verify the quality of the captured sample. If quality is adequate, system extracts features and stores them in the database. In the verification process features from fingerprint are extracted and compared with those stored in the database. The user is successfully identified when it comes to pattern matching.

A biometric recognition system can operate in two modes: verification and identification. Verification accepts or rejects the identity claim of a person. Identification determines which of the registered persons a given biometric data corresponds to.

We use verification to increase the level of security, which means that the user first enters a unique PIN number that was previously chosen when registering. Verification is also termed *one-to-one matching*.

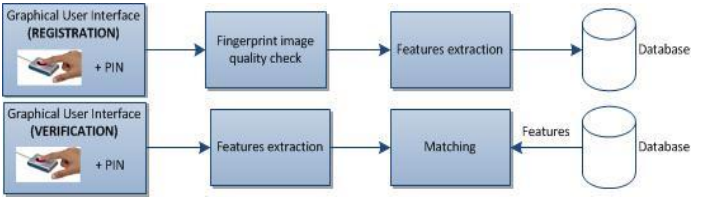

Figure 1. Simplified block diagram of registration and verification.

B. Integration in a cloud platform

A review of some existing market solutions [4,5,8] in the field of biometrics in the cloud showed some common points between the solutions. All solutions operate on the principle of the client-server model. Client on the user's computer is responsible for capturing biometric sample and sending it to the server, where matching process is executed. For the safety of network traffic between client and server security protocols are used.

Verification process is done using the following scenario (Figure 2): First, fingerprint is captured via fingerprint scanner. Scanner libraries that allow you to capture the image must be integrated into the application (web, desktop). Application communicates with API, which is hosted in the cloud. Encoded image is sent to the fingerprint processing library via API. Image is then processed in the cloud and results are sent back to the application.

Solution is modularly designed, thus upgrading is possible. Our API solution could be used for other biometric modalities, also in the context of multi-modal person authentication.

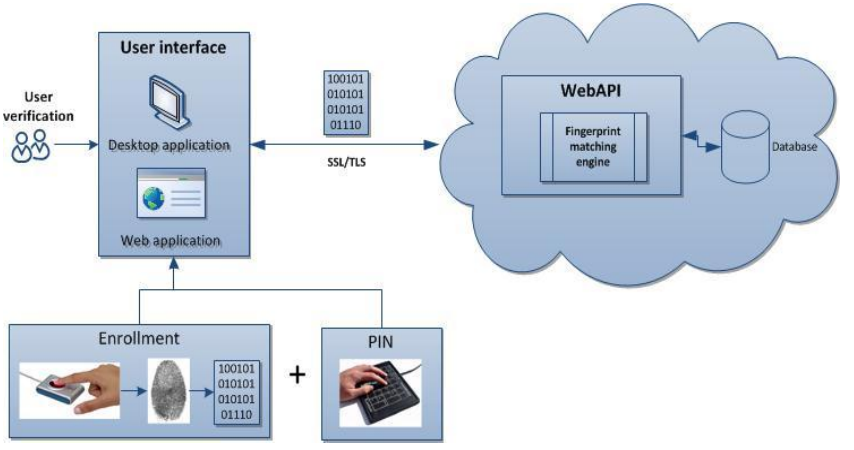

Figure 2. Scheme of the verification system in the cloud.

C. Authentication data fusion and data security

With data fusion we want to integrate multiple data derived from different authentication processes into useful representation. We combine authentication data from desktop application and data obtained from other web applications, such as Moodle [7].

Security of our solution is provided on different levels, the most important of these are: The use of HTTPS protocol for data transfer, encryption of passwords and other data in the database, access to cloud services is protected with a complex 40-digit password. However, in future work we want to implement additional security mechanisms, both in terms of storage and data transfer.

D. E-learning environment with fingerprint verification

As a proof-of-concept of biometric verification system in a cloud, we use e-learning environment Moodle [7]. Main purpose of the integration is to provide an additional level of security with an option of a fingerprint authentication as shown in Figure 3.

Overview of the pilot system is presented in Figure 4.

The main problem we face here is the integration compatibility of various fingerprint readers into different browsers. Each manufacturer of fingerprint readers offers their own protocols and libraries to access their hardware. A standard is not available yet.

Our solution uses an ActiveX component to access the hardware. ActiveX components are officially supported only in Internet Explorer, which represents a weakness in the implementation. Therefore, we want to extend the solution to work with other browsers too.

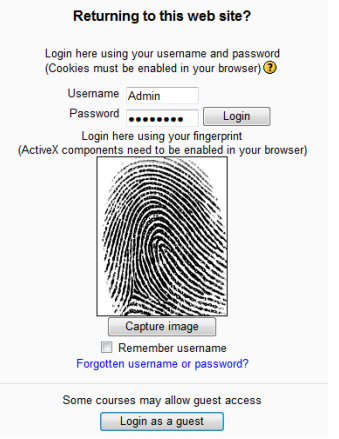

Figure 3. Customized Moodle login.

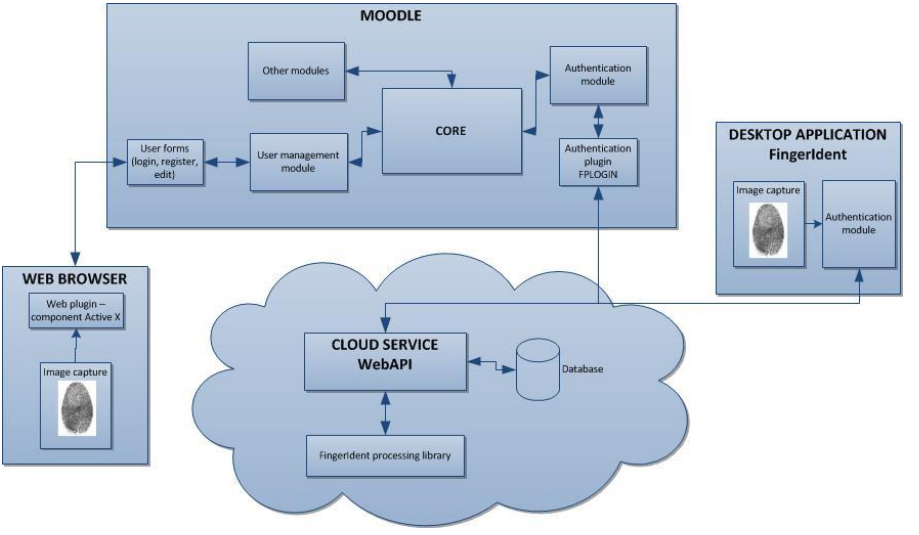

Figure 4. Cloud verification in Moodle.

III. CONCLUSION

The primary goal of our project is a working fingerprint-based biometric verification in a cloud platform. Proposed solution can be easily applied to different biometric modalities. We already installed a pilot version of the entire system, but there are many challenges left that we have to address in the future.

ACKNOWLEDGEMENTS

The work presented in this paper was supported by the European Union, European Regional Fund, KC CLASS and companies Mega M d.o.o. and Miel d.o.o.

REFERENCES

[1] D. Balfanz, et al., "The future of authentication", *IEEE Security & Privacy*, 2012, vol. 10, pp. 22-27.

[2] E. Kohlwey, et al., "Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems", *IEEE World Congress on Services*, 2011, pp. 597-601.

[3] M. Tovšak, J. Bule, P. Peer, "Upgrading a system for verification based on fingerprints", *Electrotechnical and Computer Science Conference (ERK)*, 2011, vol. B, pp. 135-138. (in Slovenian)

[4] (2012) BioID Web Services. Available at: http://www.bioid.com/products/bws.html.

[5] (2012) Ceelox ID Online. Available at: http://www.ceelox.com/ceeloxidonline.html.

[6] (2012) KC CLAAS. Available at: http://www.kc-class.eu.

[7] (2012) Moodle, open-source e-learning software platform. Available at: http://moodle.org.

[8] (2012) PasswordBank IDaaS. Available at: http://www.passwordbank.com/passwordbank-private-cloud.

[9] (2012) Slovenian Information Commissioner, biometrics. Available at: https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/. (in Slovenian)