Building Cloud-based Biometric Services

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

Jerneja Žganec Gros and Vitomir Štruc[1]
Alpineon d.o.o., Ulica Iga Grudna 15, SI-1000, Slovenia
[1]Faculty of Electrical Engineering, University of Ljubljana, Tržaška cesta 25, SI-1000, Slovenia
E-mail: {vitomir.struc, jerneja.gros}@alpineon.com

Keywords: biometrics, cloud computing, cloud integration, SaaS, fingerprint recognition

Received: December 4, 2012

Over the next few years the amount of biometric data being at the disposal of various agencies and authentication service providers is expected to grow significantly. Such quantities of data require not only enormous amounts of storage but unprecedented processing power as well. To be able to face this future challenges more and more people are looking towards cloud computing, which can address these challenges quite effectively with its seemingly unlimited storage capacity, rapid data distribution and parallel processing capabilities. Since the available literature on how to implement cloud-based biometric services is extremely scarce, this paper capitalizes on the most important challenges encountered during the development work on biometric services, presents the most important standards and recommendations pertaining to biometric services in the cloud and ultimately, elaborates on the potential value of cloud-based biometric solutions by presenting a few existing (commercial) examples. In the final part of the paper, a case study on fingerprint recognition in the cloud and its integration into the e-learning environment Moodle is presented.

Povzetek: Predstavljene so metode za biometrično razpoznavanje oseb, realizirane v oblaku.

1 Introduction

When talking about Internet authentication, in most cases, people are still talking about passwords. One of the biggest problems with current authentication approaches is the existence of too many password-account pairings for each user, which leads to forgetting or using the same username and password for multiple sites [1]. A possible solution to this problem can be found in the use of biometrics [2]. Biometric authentication techniques, which try to validate the identity of an user based on his/her physiological or behavioral traits, are already quite widely used for local authentication purposes (for private use), while their use on the Internet is still relatively modest. The main reason for this setting is open issues pertaining mainly to the accessibility and scalability of existing biometric technology.

Similar issues are also encountered in other deployment domains of biometric technology, such as forensics, law-enforcement and alike. For example, according to [3], the biometric databases of the Federal Bureau of Investigation, the US State Department, Department of Defense, or the Department of Homeland Security are expected to grow significantly over the next few yours to accommodate several hundred millions (or even billions) of identities. Such expectations make it necessary to devise highly scalable biometric technology, capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power.

The first solution that comes to mind with respect to the outlined issues is moving the existing biometric technology to a cloud platform that ensures appropriate scalability of the technology, sufficient amounts of storage, parallel processing capabilities, and with the widespread availability of mobile devices also provides an accessible entry point for various applications and services that rely on mobile clients. Hence, cloud computing is capable of addressing issues related to the next generation of biometric technology, but at the same time, offers new application possibilities for the existing generation of biometric systems [4], [5].

However, moving the existing biometric technology to the cloud is a nontrivial task. Developers attempting to tackle this task need to be aware of:

- the most common challenges and obstacles encountered, when moving the technology to a cloud platform,

- standards and recommendations pertaining to both cloud-based services as well as biometrics in general, and
- existing solutions that can be analysed for examples of *good practices*.

This paper tries to elaborate on the above listed issues and provide potential developers with some basic guidelines on how to move biometric technology to a cloud platform. It describes the most common pitfalls encountered in the development work and provides some directions for their avoidance. Additionally, it presents a case study on fingerprint recognition in the cloud, where the presented guidelines are put into action. The main motivation for the paper stems from our own work in the field of cloud-based biometric services[1] and the fact that the available literature on this field is extremely limited.

The rest of the paper is structured as follows. In Section 2 the existing literature pertaining to biometrics in the cloud is surveyed and differences with this paper are highlighted. In Section 3 some basic characteristics of cloud computing, biometrics, and cloud-based biometric services are presented. In Section 4 issues to consider when developing cloud-based biometrics are elaborated on. In Section 5 a case study on fingerprint recognition in the cloud is presented and, finally, the paper is concluded with some final comments and directions for future work in Section 6.

2 Related work

Cloud computing is a highly active field of research and development, which gained popularity only a few years ago. Since the field covers a wide range of areas relating to all levels of cloud computing (i.e. PaaS, IaaS, and SaaS), it is only natural that not all possible aspects of the field is appropriately covered in the available scientific literature. This is also true for cloud-based biometrics.

While there are some papers addressing this topic, they are commonly concerned with specific aspects of the technology and neglect the bigger picture. The work of Gonzales et. al [7], for example, addresses cloud-based biometrics, but focuses on how to protect biometric data from miss-use through a crypto-biometric system. A similar topic is also discussed by Vallabhu and Satyanarayana in [8]. Other researchers focus more on developing biometric technology for a certain biometric modality and present cloud computing as a possible use-case [9], [10]. This paper, on the other hand, tries to cover different aspects of cloud-based biometrics and is equally interested in legal (e.g., issues relating to data protection, data retention etc.) as well as technical issues. From this point of view, the topic of the paper is more closely related to the work of Senk and Dotzler [11] or Kohlwey et. al [12], where biometrics and cloud computing are also discussed in a broader context in addition to presenting a case study on a specific modality.

3 Biometrics and cloud computing

3.1 Cloud computing

Cloud computing is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion [13].

NIST defines five key characteristics of cloud computing [14]:

- *Rapid elasticity* - elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing as needed [14].
- *Measured services* – certain aspects of the cloud service are controlled and monitored by the cloud provider. This is crucial for billing, access control, resource optimization, capacity planning and other tasks [14].
- *On-demand self-service* - a consumer can use cloud services as needed without any human interaction with the cloud provider [14].
- *Ubiquitous network access* - the cloud provider's capabilities are available over the network and can be accessed by various clients through standard mechanisms [14].
- *Resource pooling* - allows a cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location [14].

Clearly, cloud computing has several desirable characteristics, which make the cloud platform highly suitable for various applications, including biometrics.

3.2 Biometric systems

Biometric recognition systems represent pattern recognition systems, capable of recognizing individuals based on their physiological or behavioural traits [2]. These traits are considered to be unique to each individual and unlike knowledge or token-based security mechanisms cannot be forgotten, lost or stolen. The most common traits used for biometric recognition are: faces, fingerprints, irises, palm-prints, speech etc.

[1] Conducted in the scope of the KC CLASS (CLoud Assisted ServiceS) project. [6]

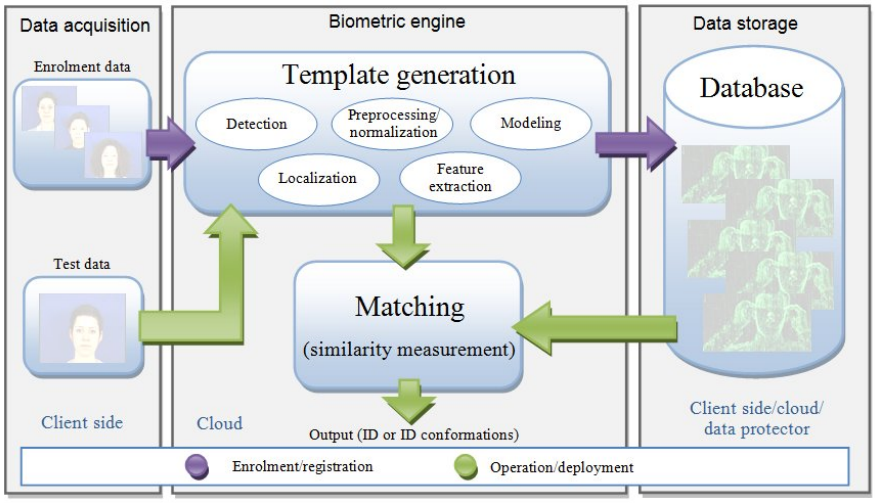

Figure 1: Block diagram of a typical biometric recognition system.

Biometric systems typically conduct one of two tasks: *identification* or *verification/authentication*. The verification/authentication task tries to validate the identity claim of the user currently presented to the system, while the identification task tries to determine, which of the registered user the acquired "live" biometric sample corresponds to. Hence, the identification problem is commonly considered to be a one-to-N matching problem, while the verification/authentication problem is considered to be a one-to-one matching problem.

Biometric systems always comprise the same basic components regardless of whether they are designed for the cloud or any other platform. These components, which are also shown in Fig. 1 for the case of a face recognition system, include [2], [4]:

i) *a data acquisition component* (or sensor) that captures a still image or video sequence of a user trying either to enrol into the system or to use the system for authentication/identification purposes,

ii) *a template generation component* that uses machine learning, computer vision and pattern recognition techniques to derive a biometric template from the input data,

iii) *a database of biometric templates* belonging to enrolled/registered users, and

iv) *a matching component* that compares the biometric template derived from the "live" image with the appropriate template(s) stored in the database of the system and based on the outcome makes a decision regarding the identity of the user currently presented to the system.

While the basic layout of a biometric recognition system is more or less the same on any platform (and biometric modality), there are, however, a number of aspects that are specific to the cloud. These aspects will be discussed in more detail in the next section.

3.3 Biometrics in the cloud

As emphasized in the previous section, there are certain aspects of biometric systems that are specific to cloud computing. First of all, the biometric engine[2] is located in the cloud and not on some local processing unit, as it is the case with traditional (e.g. access control) biometric recognition systems. This characteristic makes the cloud-based biometric technology broadly accessible and provides the necessary means for integration in other security and/or consumer applications. Second of all, storing biometric data in the cloud makes the system highly scalable and allows quick and reliable adaptation of the technology to an increasing user base [3].

On the other hand, storing biometric data in the cloud may raise privacy concerns and may not be in accordance with national legislation. Last but not least, a cloud implementation of biometric technology may harvest all merits of the cloud, such as real-time and parallel processing capabilities, billing by usage etc. [3]. All of the presented characteristics make cloud-based biometric recognition technology extremely appealing.

When developing biometric technology for the cloud, one needs to make a number of design choices. Probably the most important choice is, which components to move to the cloud and which to implement locally. A review of some existing market solutions ([15], [16], [17], [18], [19]) from the field of cloud-based biometrics reveals that most often both the biometric engine as well as the biometric database is moved to the cloud. The commercial solutions typically operate on the principle of the client-server model. The local client (e.g. on the user's computer) is responsible for capturing a biometric sample of the user and sending it to the server (hosted in the cloud), where the matching process is executed. For the safety of the network traffic between the client and the server designated security protocols are commonly used.

[2] We will refer to the template generation and matching components as the biometric engine in the remainder of the paper.

While the presented configuration makes full use of the merits of the cloud platform, it may not be conformant with the local legislation. Therefore, the possibility of using a locally hosted database needs to be considered when designing a cloud-based biometric system. Such a setting may limit the scalability of the technology to a certain extent, but is reasonable as it makes potential market-ready technology more easily adjustable to currently existing legislation. Another possible solution to the legislation problem could also be found in the use hybrid clouds.

4 Integrating biometrics in the cloud

4.1 Challenges and obstacles

When developing biometric technology for the cloud, one inevitably encounters a number of challenges and obstacles that need to be addressed. Next to meeting performance criteria and selecting the most suitable platform for the development work, current legislation pertaining to cloud computing and biometrics in general, privacy concerns and data protection issues all represent major challenges for the development process [4].

The challenges pointed out above are addressed in different ways. The performance of the biometric recognition technology can systematically be evaluated using established reproducible scientific methodology. Here, publicly available databases with predefined experimental protocols and performance criteria are typically employed to produce performance estimates that can be compared with performance estimates of previously assessed technology.

The platform used in the development work is commonly selected according to ones preferences or with respect to the planned characteristics of the final product (i.e. deployable in a private or public cloud etc.).

When it comes to legal, privacy and data protection concerns, there are usually no universal solutions, as they differ from country to country. In the case of Slovenia, for example, the information officer has composed several guidelines/recommendations both for the cloud as well as biometric technology. The recommendations relating to biometric technology, biometric data protection and template storage can be found in [20] and fall in the domain of ZVOP-1 (in Slovenian: *Zakon o varstvu osebnih podatkov*), while the guidelines for cloud computing are accessible from [21].

4.2 Standards and recommendations

There are several standards and recommendations that are relevant in the context of both biometric recognition as well as cloud computing. These include internet protocols, data formats, communication and security protocols, recommendations for cloud application design, recommendations for biometric technology design etc. Since this field is too broad to be covered completely, the focus of this paper is only on a small number of important standards related to biometric recognition technology in the cloud.

The first group of standards of interest for every developer working in the field of biometric recognition are standards that allow for interoperability among different vendors (e.g. [22], [23]). These standards define interchange formats for biometric data and (next to interoperability) also enable consolidation of different biometric databases. The standard in [23], for example, specifies interchange formats for face images and as such defines full-frontal and token face images (defined by the location of the eyes) and ensures that enrolled images meet a sufficient quality standard for arbitrary face recognition technology. Similar standards also exist for other biometric traits [24].

The second group of standards of relevance to cloud-based biometrics is the OASIS standard for Biometric Identity Assurance Services (BIAS) [25]. The open standard defines all specifications for SOAP-based biometric services and is conveniently supported by a reference implementation (for fingerprints) provided by NIST. The ISO/IEC JTC 001/SC 37 has just recently approved a project to internationalize the above mentioned BIAS standard.

4.3 Deployment possibilities and existing solutions

Cloud-based biometric technology offers attractive deployment possibilities, such as smart spaces, ambient intelligence environments, access control applications, mobile application, and alike. While traditional (locally deployed) technology has been around for some time now, cloud-based biometric recognition technology is relatively new. There are, however, a number of existing solutions already on the market, these include (among others) the solutions by Animetrics [15], BioID [16] and, of course, Face.com [17], which has recently been acquired by Facebook.

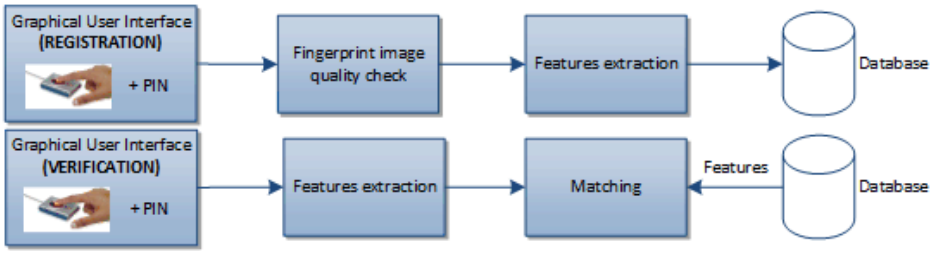

Figure 2: Simplified block diagram of biometric registration and verification.

5 A case study: fingerprint recognition in the cloud

5.1 Goal and setup

The goal of the case study presented in the remainder is to put the general guidelines presented in the previous sections into practice and provide more detailed (technical) information on the process of integrating biometric technology into a cloud platform. The basis of the case study represents a prototype fingerprint recognition systems, named FingerIdent [26]. A local test version of this prototype system is already installed at the Faculty of Computer and Information Science, University of Ljubljana, in front of the Computer Vision Laboratory.

The functionality of the existing local version of the FingerIdent system can be divided into two main categories:

i) *user registration (enrollment)*, during which a biometric template of a given user is constructed and stored in the system's database, and

ii) *user verification*, during which the identity claim of a given user is validated.

The registration process uses a fingerprint reader to capture the (biometric) fingerprint data. In the next phase the quality of the captured sample is evaluated and if it is found to be adequate, the system extracts features from it and stores them in the form of a biometric template in the database. During the verification process features from the captured "live" fingerprint are again extracted and compared to those stored in the database. The comparison is made based on pattern matching procedures, which form the foundation for the validation of the identity claim. An illustration of both functions is shown in Fig. 2.

To reach the goal of devising a cloud-based biometric service, one needs to migrate the presented functionality of the local FingerIdent system to the cloud and provide the necessary infrastructure for accessing the biometric service. Details on this procedure are given in the next section.

5.2 Designing cloud biometric services

It was emphasized in Section 3.3 that a decision has to be made with respect to which components of the biometric system should be moved to the cloud and which implemented locally. For our case study, we decided to move the biometric engine as well as the biometric database to the cloud. A block diagram of the complete cloud-based biometric service design is shown in Fig. 3.

Note that the verification process with the described design is conducted using the following scenario:

i) the fingerprint of a given user is first captured via a fingerprint scanner (here scanner libraries that allow capturing fingerprint images need to be integrated into the local (desktop or/and web) application);

ii) the application then communicates through a (REST) API with the biometric web service hosted in the cloud and sends an encoded image to the fingerprint processing library (i.e. FingerIdent library) that provides the functionality for the cloud service;

iii) the transmitted fingerprint image is processed in the cloud and finally the result is sent back to the local application.

The security of the presented solution is provided on different levels through:

- the use of the HTTPS protocol for data transfer,
- the use of certificates (the SSL protocol),
- the encryption of passwords and other data (such as biometric templates) in the database, and
- the protection of the access to the cloud-service with a complex 40-digit password.

The cloud-based service is designed modularly, which makes upgrading the service a relatively simple task. Equally important is the fact that the same design is also suitable for other biometric modalities and allows for devising multi-modal person authentication as well.

5.3 Moodle with fingerprint verification

To demonstrate the effectiveness of the presented solution and to provide a proof-of-concept, the e-learning environment Moodle [27] is augmented with biometric authentication capabilities by integrating it with the cloud-based fingerprint verification service.

Since Moodle is also designed modularly, the biometric authentication procedure is implemented as an additional (optional) authentication scheme, which can complement the existing procedures and provide an additional level of access security. A block diagram of the integration is shown in Fig. 4.

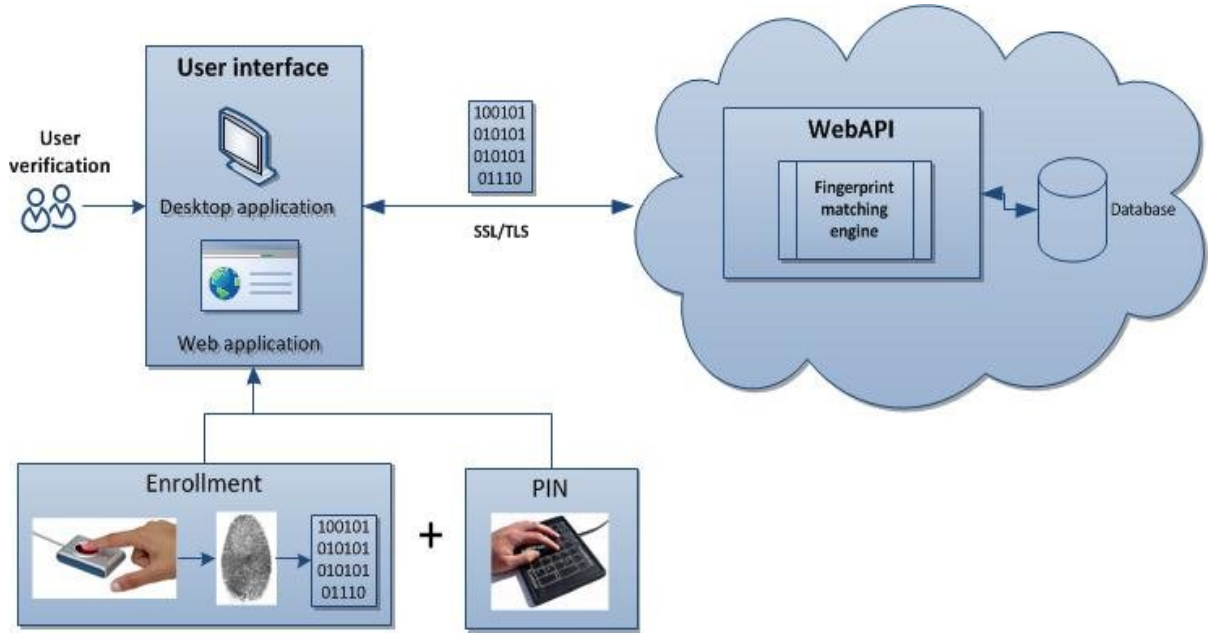

Figure 3: Scheme of the biometric verification system in the cloud.

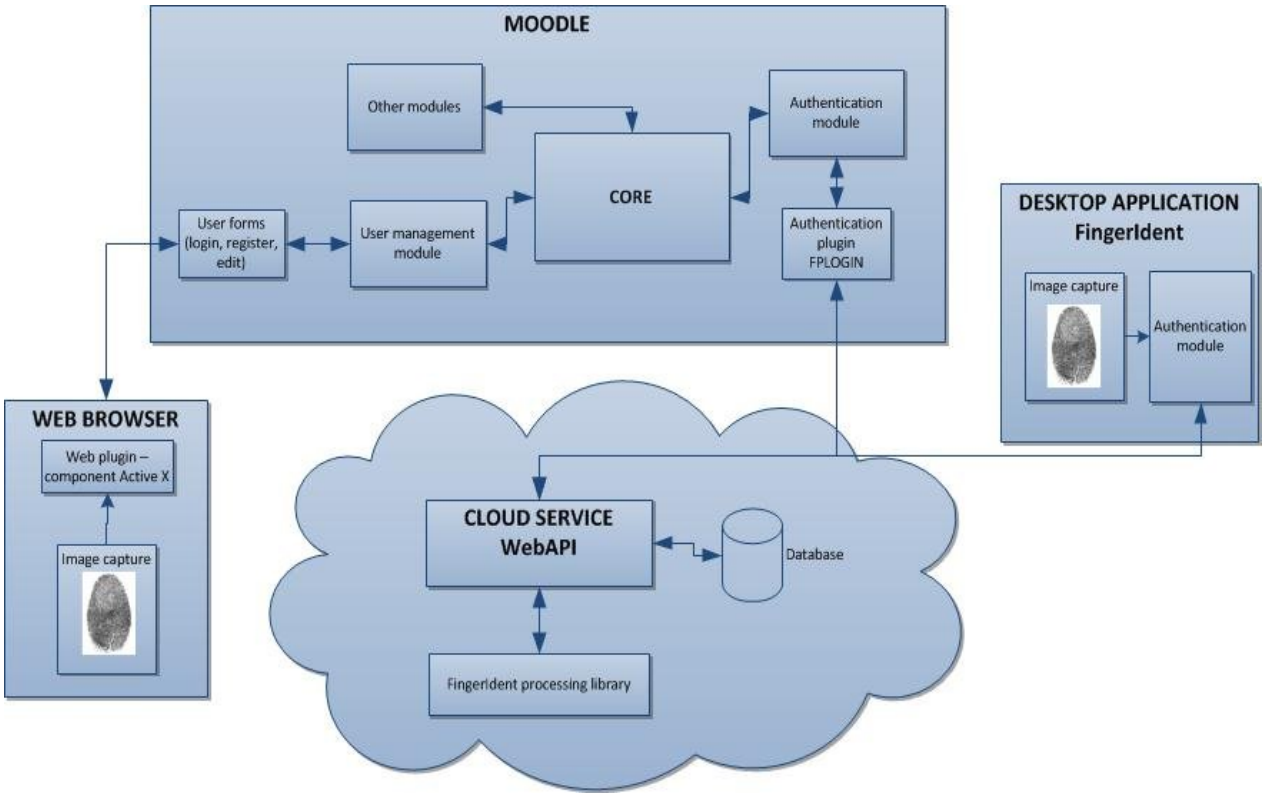

Figure 4: Cloud fingerprint verification in Moodle.

The main problem faced during integration is the compatibility of various fingerprint readers with different browsers. Each manufacturer of fingerprint readers offers their own protocols and libraries to access the corresponding hardware. A standard is not yet available.

The solution developed in the scope of this case study uses an ActiveX component to access the hardware. ActiveX components are officially supported only on Internet Explorer, which represents a weakness in the implementation. As future work, an extension of the presented solution is planned, so it can work with

other popular browsers, such as Firefox, Opera or Chrome too.

After the integration of the fingerprint authentication service into the Moodle framework, the Moodle login screen was modified to account for the added functionality. The result of this procedure is shown in Fig. 5. Note how the added biometric authentication functionality seamlessly integrates into the existing framework.

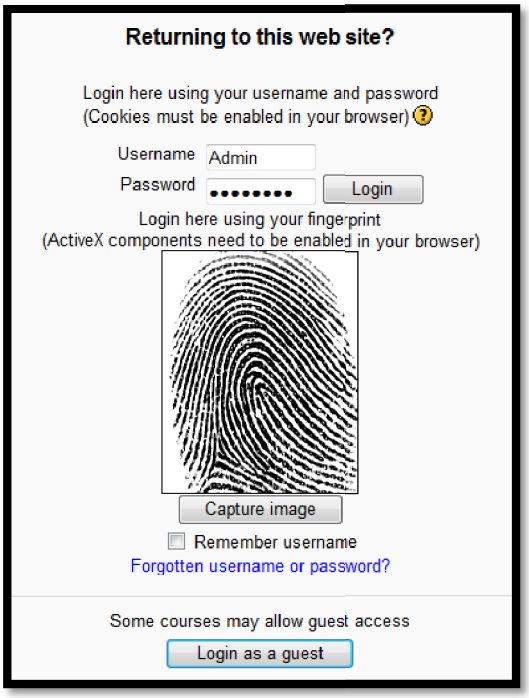

Figure 5: Customized Moodle login.

6 Conclusion

Cloud based biometric services have an enormous potential market value and as such attract the interest of research and development groups from all around the world. In this paper some directions on how to move existing biometric technology to a cloud platform were presented. Issues that need to be considered when designing cloud-based biometric services have been presented and a case study, where a cloud-based fingerprint service was developed and integrated with the e-learning framework Moodle was described as well. As part of our future work we plan to migrate more biometric modalities to the cloud and, if possible, devise a multi-modal cloud-based biometric solution

Acknowledgements

The work presented in this paper was supported by the European Union, European Regional Fund, within the scope of the framework of the Operational Programme for Strengthening Regional Development Potentials for the Period 2007-2013 contract No. 3211-10-000467 (KC Class), the postdoctoral project BAMBI with ARRS ID Z2-4214.

References

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

[2] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.

[3] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud for Big Data Biometrics: Meeting the performance requirements of the Next Generation Biometric Systems," in *Proceeding of the IEEE World Congress on Services*, pp. 597-601, 2011.

[4] V. Štruc and J. Žganec-Gros, "Developing Face Recognition Technology for the KC Class Biometrics service," in: *CLASS Conference 2012*, pp. 68-75, 2012.

[5] J. Bule and P. Peer, "Fingerprint Verification as a Service in KC CLASS," in: *CLASS Conference 2012*, pp. 76-82, 2012.

[6] The KC Class project, available from: http://www.kc-class.eu/, last visited: 5.12.2012.

[7] D. Gonzales Martinez, F.J. Gonzels Castano, E. Argones Rua, J.L. Ala Castro, D.A. Rodriguez Silva, "Secure Crypto-Biometric System for Cloud Computing," in: *International Workshop on Securing Services on the Cloud*, pp. 38-45, 2011.

[8] H. Vallabhu and R.V. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," *International Journal of Soft Computing and Engineering*, vol. 2, no. 4, pp. 163-165, 2012.

[9] S. Suryadevara, S. Kapoor, S. Dhatterwal, R. Naaz and A. Sharma, "Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security," in: *International Conference on Information and Network Technology*, vol. 4, 2011.

[10] S.N.S. Raghava, "Iris Recognition on Handoop: a Biometrics System Implementation on Cloud Computing," in: *Proceedings of IEEE CCIS,* 2011.

[11] C. Senk and F. Dotzler, "Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Perspective," in: *International Conference on Availability, Reliability and Security*, pp. 43-50, 2011.

[12] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems," in: *IEEE World Congres on Services,* pp. 597-601, 2011.

[13] D.M. Dakhane and A.A. Arokar, "Data Secuity in Cloud Computing for Biometric Application," *International Journal of Scientific & Engineering Research*, vol. 3, no. 6, pp. 1-4, 2012.

[14] Cloud computing use case discussion group, "Cloud Computing Use Cases: White Paper" available from: http://cloudusecases.org/, last visited: 05.12.2012.

[15] Homepage of the Animetrics cloud-based face recognition solution, available from:

http://animetrics.com/cloud-face-recognition-services/, last visited: 03.10.2012.
[16] Homepage of the BioID cloud-based biometric recognition solution, available from: http://www.bioid.com/, last visited: 03.10.2012.
[17] Homepage of the Face.com cloud-based face recognition solution, available from: http://face.com/, last visited: 03.10.2012.
[18] Homepage of Ceelox ID Online, available from: http://www.ceelox.com/ceeloxidonline.html, last visited: 05.12.2012.
[19] Homepage of PasswordBank IDaaS, available from: http://www.passwordbank.com/passwordbank-private-cloud, last visited: 05.12.2012.
[20] Homepage of the Slovenian Information Commissioner, biometrics, available from: https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/, last visited: 03.10.2012.
[21] Information Commissioner, Cloud Security Alliance Slovenia Chapter, Slovenski institut za revizijo, Slovenski odsek ISACA, Zavod e-Oblak, Eurocloud Slovenia, "Varstvo osebnih podatkov & računalništvo v oblaku," pp. 31, 2012, available from: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf, last visited: 03.10.2012.
[22] Information technology, "Biometric data interchange formats – Part 5: Face image analysis," *Documents ISO/IEC 19794-5:2005*, 2004, available from: http://www.iso.org, last visited: 03.10.2012.
[23] Information technology, "Face recognition format for data interchange," *Document 385-2004 ANSI INCITS*, 2004, available from: http://www.iso.org, last visited: 03.10.2012.
[24] NIST standard, ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, available from: http://www.nist.gov/itl/iad/ig/ansi_standard.cfm, last visited: 03.10.2012.
[25] OASIS standard, "Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0," pp. 210, May 2012, available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bias, last visited: 03.10.2012.
[26] M. Tovšak, J. Bule, P. Peer, "Upgrading a system for verification based on fingerprints," in: *Electrotechnical and Computer Science Conference (ERK)*, vol. B, pp. 135-138, 2011.
[27] Moodle, open-source e-learning software platform, available from: http://moodle.org, last visited: 06.12.2012.