Computer Science and Information Systems 13(2):313–334 DOI: 10.2298/CSIS141030003J

Extending identity management system with multimodal biometric authentication

Bojan Jovanović[1], Ivan Milenković1, Marija Bogićević Sretenović[1], and Dejan Simić[1]

[1] University of Belgrade, Faculty of Organizational Sciences, Jove Ilića 154, 11000 Belgrade, Serbia
{bojan.jovanovic, ivan.milenkovic, marija.bogicevic, dejan.simic}@fon.bg.ac.rs

Abstract. Techniques for authentication that are used in today's identity management systems are vulnerable when they are used over the network. In order to prevent fraud and unauthorized data access, it is important to ensure the identity of the person who submitted authentication credentials. The authentication process can be additionally secured by using biometric data for user verification. Moreover, precision of biometric authentication can be improved by the use of multimodal biometrics. This paper presents a system which has been designed for identity management based on FreeIPA solution for digital identity management and MMBio framework for multimodal biometrics. Proposed system provides multifactor authentication, where MMBio framework is used for handling user biometric data. Developed prototype confirms possible integration of identity management and multimodal biometric systems.

Keywords: identity management system, authentication, multimodal biometrics, open source

1. Introduction

Modern information technologies have enabled information infrastructure to connect remote entities around the world by using large networks, relying on application level protocols and web services. The advantages of computing resources, which are available on the Internet via cloud computing and virtualization technologies, are being used by the companies to an increasing extent. Given that the number of online users is constantly growing [1], the issue of digital identity management arises in order to protect privacy and retain liabilities in transactions and interactions in accordance with the regulatory controls.

Digital identity can be defined as the digital representation of information about a particular person or organization. Digital identity has a finite, but also an unlimited number of attributes [2]. Digital identity may include attributes of a person such as: name and surname, personal identification number (PIN) or passport number. Additionally, it can obtain biometric data such as the iris of the eye or a fingerprint, as well as the information about the users' activities, including web searches and transactions during Internet purchase.

The identity management and access control involve several fundamental parts, such as: user identification, authentication and authorization. These three activities are

strongly connected and, in fact, we can say that they form a chain of interdependence. Authorization depends on authentication, and the authentication itself is based on identification [3]. There are lot of other activities that are important for identity management, but particular emphasis is put on managing user accounts and monitoring of the system user activities.

Biometric authentication establishes a person's identity based on something she is, rather than something she possesses or remembers [4]. As tokens can be stolen or lost, and passwords misremembered or compromised, this is a significant advantage. However, algorithm used for biometric recognition are based on representations of biometrical data – biometrical characteristics. Even two samples of biometric data gathered from the same person are never the same, due to sensor noise, aging and imperfect acquisition conditions[5]. Therefore, there is always a possibility of biometric system error. Multimodal biometrics is a possible solution for improving biometric system precision [4]. In multimodal biometrics, different modalities are taken simultaneously in order to determine users' identity.

In order to respond to current trends, a prototype system for identity management needs to be developed. It is necessary that this system fulfils requirements for identity management, policies and monitoring of the system user activities. In order to have an expandable system, its basic components should use open source technologies. In accordance with these requirements, a system has been designed for identity management based on FreeIPA solution for digital identity management and MMBio framework for multimodal biometrics [6].

In first section an introduction to paper was given. Section 2 explains problems explored by this paper. Section 3 describes identity management concepts and solutions. In section 4 an overview of FreeIPA solution is given. Topic of section 5 is multimodal biometrics. Section 6 presents the architecture of integrated identity management and multimodal biometric system. In section 7, a description of integrating multimodal biometrics into FreeIPA solution is given. Section 8 describes Multimodal Biometric Matcher (MMBio matcher). Section 9 describes system deployment and possible applications. In section 10, evaluation of deployed system is given. Conclusions and suggestions for future work are given in section 11.

2. Problem Statement

Commonly used authentication methods, such as passwords and tokens have some limitations. Neither passwords nor tokens guarantee that the person who entered the password or presented the token is its legitimate owner. Therefore, a security risk is present in any system based on passwords or tokens.

A possible alternative to these authentication methods is the use of biometrics. Biometric authentication depends on something that person is, rather than something she knows or possesses. However, the use of biometrics raises several challenges.

Currently used biometric methods do not guarantee absolute precision [4]. Although it may be very low, there is always a chance that a biometric system may incorrectly refuse to authenticate legitimate user, or wrongly accept imposters. Some biometric modalities have higher error rates. For example, authentication solely based on behaviouristic modalities such as voice or gait, is still not a feasible option.

Commercial biometric solutions are costly. A possible alternative is the use of open-source solutions. These solutions often have lower precision than their commercial counterparts [5]. It is possible to improve their precision by using multimodal or multibiometric approaches. However, they are often developed in different programming languages, for different operating systems, and do not support standard interoperability mechanisms.

Biometric data is irrevocable [7]. Some algorithms for revocable biometrics exist, but they seriously affect verification precision. Therefore, there is a need for extra layer of security, because if an attacker compromises raw biometric data, it cannot be replaced.

Commercial solutions are often based on local feature extraction and matching on device. For example, some mobile phones and laptops have a fingerprint reader with integrated feature extraction and matching. Although such approach increases system security, it is unfeasible when distributed databases are present. Police and government databases are among such examples.

Authentication is just one among many functionalities of an identity management system. It is often unfeasible to develop and implement a new system solely because an alternative authentication method is being used. Many organizations and companies use Linux/Unix environment with its underlying services [8]. As a consequence, biometric authentication should be integrated in existing solutions. It is necessary to have broad, system approach when performing such integration, as there are both challenges on the client and the server side of the identity management solutions.

In order to solve these challenges, we have extended FreeIPA identity management system with multimodal biometric authentication. To implement multimodal biometric authentication, we have developed MMBio framework, solution for integrating unimodal biometric solutions into a multimodal biometric system. Our system proposal is presented in section 6, while MMBio framework and biometric authentication are described in sections 7 and 8.

3. Identity Management

Identity management can be defined as the creation, management and use of digital identities [9]. Identity management implies safe management of the entire digital identity's lifecycle, from its creation (registration of a digital identity), through maintenance (implementation of organizational policies with regard to the access to electronic resources) and, eventually, the termination of digital identity. It allows efficient and safe access to data and applications.

Three key elements of identity management are: policies, processes and technology. Policies refer to limitations and standards that need to be followed in order to be in compliance with regulations and business practices. Processes describe the sequence of steps that lead to the completion of business tasks or functions. Technologies are automated tools that help achieve business goals more efficiently and accurately with regard to all limitations and guidelines outlined in the policy.

Identity management system of an organization does not remain stagnant over time. New technologies will be introduced into the system, new business models and limitations will change the processes and management type. Once one of the elements undergoes a change, a new balance needs to be established [10].

- Basic concepts of digital identity are:
- The subject, entity
- Resource
- Digital identity
- Authentication
- Authorization
- Federation
- Integrity
- Single sign-on (SSO)

The subject or an entity is a person, group of people, an organization, a virtual object (e.g., computer process, application, text file), tangible object (e.g., electrical appliances and computers) or any other entity that requires access to a particular resource. A resource can be a specific data in the database, a remote server or a website, and what is common to all the resources is the access, i.e., the entity refers to its own digital identity when accessing the resource.

Digital identity, the very concept of it, represents an experience of one's' own identity, the identity of other people and things in the aspect of digital technologies [11]. The definition of digital identity consists of the following parts:

- Identifier
- Credentials
- Key attributes
- Context-specific attributes

The identifier or the key is a part of the information that uniquely identifies the object in a particular context. Examples of identifiers are email addresses, user names or the unique identification number that every person possesses. Credentials are private or public data that could be used as proof of identity authentication.

Key attributes represent data that help describe identity. Key attributes can be used in a variety of different business and application contexts. For example, addresses and phone numbers are common attributes used in a variety of business application. Context-specific attributes are data that help describe the identity, but these attributes are used only in specific contexts.

Authentication is a process of verifying the identity of the user, devices, or other entity in a computer system, which is often a prerequisite for gaining access to system resources.

Authorization is an approval given to the user, application program or a process to accesses a particular object or group of objects. Authorization is often resolved through the mechanism of roles. It is possible to assign a specific role or group of roles to one user or a group of users. The role may consist of other roles, which together make up a set of privileges at the disposal of the authorized entity.

Federation enables secure sharing of information with external systems that need to manage the identities of foreign users[12]. Without this functionality, administrators would have to maintain a separate folder for all foreign users and manually update data about them [13]. Identity Federation represents a circle of trust and allows users from one domain to access resources in another domain without any additional introduction.

Integrity is a guarantee that the content of the received message was not altered in respect to the content of the original message sent.

Single Sign-On (SSO) is a process of authentication that allows a user to access one or more resources within single security domain. SSO is a common procedure in Enterprises, where clients logs in once and gain access to different resources connected to a local area network (LAN), without the need to re-enter log-in credentials.

3.1. Identity management systems

The solution offered by Microsoft, Active Directory Services (ADS), includes an integrated identity management system. Ever since the Windows server 2003 R2, Active Directory Federation Service (AD FS) is an integral part of the ADS and is being used to create connections between organizations. This is possible by user authentication through Active Directory which represents an identity provider. Moreover, AD FS issues tokens that are used in the authentication process. In addition to ADS, Microsoft has also developed MIIS-Microsoft Identity Integration Server, which has changed names, but in the year 2010 was presented as FIM – Forefront Identity Manager. FIM was developed in order to integrate with Active Directory and Microsoft Exchange solutions.

IBM offers an identity management system, which is a part of Tivoli and is called Tivoli Identity Manager, based on policies and roles [14]. It provides a hierarchy of roles, web self-services, group management and synchronization of user data with different repositories. The advantage is in the possible synchronization of Tivoli with ERP systems. Furthermore, there is a possibility of using biometrics as an authentication method.

The imposed open source solution is the FreeIPA solution that allows creation of identity storages, centralized authentication, domain control for Kerberos and DNS services and authorization policies, and all this on Linux systems using the native Linux tools. Basically, the FreeIPA is a domain controller for Linux and Unix systems. FreeIPA defines the domains through control of the servers and reported client machines. That provides a centralized structure that was previously unavailable in Linux/Unix environments, and all this through the use of native Linux applications and protocols.

4. FreeIPA

FreeIPA IdM system is a set of services and rules for managing users of an organization. It includes data about individuals, hosts, groups, roles, and authentication and authorization rules.

From the server side, FreeIPA consists of the following components:

- Authentication: Kerberos KDC, Dogtag Certificate System
- Data Storage: 389 Directory Server
- Server/Client Discovery: DNS(Domain Name System)
- Management: NTP (Network Time Protocol)

The main responsibilities of the whole system can be divided into following tasks:

- Identities – where identification is represented as the key for establishing relations between objects, equality of users, hosts and services
- Authentication – both users and hosts own credentials and can authenticate each other or authenticate to each other.
- Access Control – process of enforcing access privileges within implementation of standard access controls [15].

Flexible architecture leads to a scalable system between centralized and distributed architecture. On the client side, the key components are:

- SSSD (System Security Services Daemon) – Replaces legacy clients such as PAM/pam_ldap, pam_krb5/ and NSS/nss_ldap/. These services do not have advanced features as SSSD. They still exist on the system, but are wrapped with SSSD.
- Certmonger – retrieval tool for digital certificates

Main feature of SSSD is pluggable service. It provides connector for multiple identity systems, even at the same time. Also, SSSD organizes identity information sources into "domains": FreeIPA Domains, Active Directory Domains, Plain LDAP servers, etc.

Another interesting feature of SSSD is smart caching of identity information. Smart caching can automatically refresh identity information as needed. It supports offline identity during network interruption and/or server maintenance. Also, smart caching keeps access credentials private [16].

These facts about FreeIPA as IdM, and the fact that FreeIPA is open source IdM, lead us to choose it as a good choice for research of the possible integration of multimodal biometric solution into IdM authentication process.

5. Multimodal Biometrics

Biometric authentication uses something that person is in order to establish its identity. In this way, issues with password memorization and safety of the object are resolved, and the identification of a person is enabled without external data or objects [17]. This is particularly significant once we take into consideration the fact that distance communications are expanding. Throughout the Internet people use services such as electronic commerce and administration, they perform business transactions, study and maintain personal contacts.

Similarly to the Internet technology, the first implementation of biometrics was for military purposes. Academic institutions have directed their efforts adequately with the more evident need for biometric technologies. Progress in the technology development, specifically in biometric sensors of affordable price, has enabled the implementation of biometric technology in new areas [6]. Now, even the smaller development teams with limited budget can afford the costs of procurement of appropriate equipment used for development and testing. This technology development trend has assisted the emergence of open source biometric solutions, developed by the open source community.

Potential users have at their disposal numerous commercial as well as open source solutions. Commercial solutions often make up closed units, with all the advantages and disadvantages of this approach. Some of the open source solutions enable the development of flexible systems, which can have the same use value as commercial solutions in certain situations, but with much smaller financial investments.

However, biometric solutions do not guarantee an absolutely reliable decision. Biometric relies on machine learning and statistical algorithms, and output from these algorithms is a probability or similarity score, not a definite yes/no decision [5]. There are several possible reasons for this inaccuracy. As first, noise may be present during the data acquisition phase. For example, face recognition system could be negatively affected by unfavourable lightning. As second, some biometric modalities change over time. Moreover, acquisition sensors may lack precision required for absolutely reliable authentication.

Different multibiometric approaches were implemented in order to resolve this problem. A promising multibiometric approach is the use of multimodal biometrics. Systems that integrate multiple different biometric modalities, e.g., face and fingerprint, voice and the iris, are called multimodal biometric systems.

5.1. Information Fusion in Multimodal Biometrics

Integral parts of multimodal biometric systems are methods for fusion of information gathered from different biometric modalities. Choice of the fusion algorithm can have a significant impact on the system precision and performance.

First opportunity for information fusion is at the sensor level. Data gathered from several types of sensors is integrated into single entity. At this level it is usual to fuse data from just a single biometric modality, so these methods are more likely to be considered multibiometrics than multimodal biometrics. However, as this kind of fusion can improve system inputs, it is important for consideration. More information on the topic can be found in the following work [18].

Combining biometric characteristics extracted from several biometric modalities into a single biometric characteristic is considered as fusion at feature extraction level. Fusion methods defer from simple vector concatenation to more complex fusion methods. Paper [19] describes a multimodal biometric system with feature level fusion based on Gabor-Wigner transform.

In case of score level fusion, separate biometric characteristics are generated for each biometric modality. Each of the characteristics is matched with according template in the biometric database. The result of the matching is matching score. In case of similarity scores, the greater the similarity between matched templates, the match score has the higher value. Generated match scores are used to generate new, derived match score, or are directly used to make a decision. Most of the published papers use this fusion method. Some of the papers are [20] [21].

If a biometrical system functions in the identification mode, it is possible to use rank method fusion. Such system could produce an ordered list of identities as an output. The first candidate on the list is the one system determined a most likely match, followed by the other candidates ranked by their match probabilities. Monwar and Gavrilova [22] have tested different rank based fusion methods

Some commercial unimodal biometric system function as black box systems and their only output is final decision. Integrating such unimodal systems into a multimodal recognition system requires the use of decision level fusion. Decision level fusion applies different voting algorithms to calculate the final decision. Paper [23] describes a biometric system with decision level information fusion.

6. System Architecture

Current operating systems use text password for user authentication. Almost everyone knows the weaknesses of this method of user authentication [24]. The main objective of the proposed prototype is to extend the current one-component method to authenticate users on a multi-component method to authenticate users.

As previously stated, multimodal approach to user authentication uses more biometric modalities in order to determine the unequivocal identity of the user. However, biometric solutions do not guarantee absolutely accurate recognition. When it detects user identity from a biometric sample, biometric system in response can return multiple user identities.

The process of user authentication at the operating system requires unambiguous identification of the user. Therefore, in our prototype, password is just one of the authentication methods. Its task is to unambiguously determine the identity of the user. Biometric data acquired should confirm that the password was entered by its owner.

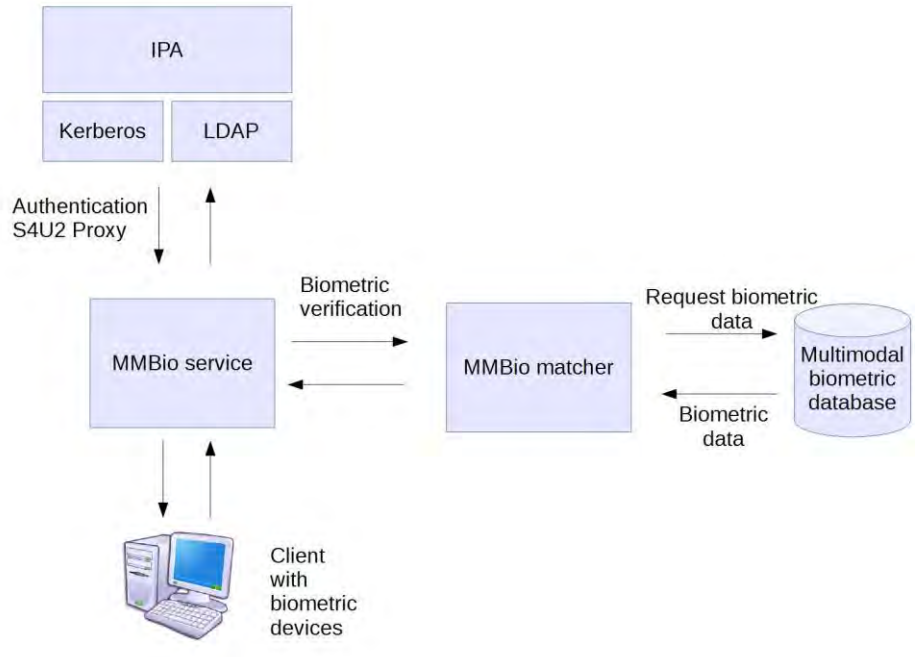

Fig. 1. MMBio server architecture

Figure 1 shows architecture of identity management solution based on FreeIPA with multimodal biometric authentication. System components are client systems, MMBio service, MMBio matcher, and FreeIPA IdM.

Client systems are equipped with FreeIPA client software and adequate biometric sensors. It is necessary for client systems to be logged on to IdM domain. During the authentication process, client sends standard credentials together with biometric samples packaged in a SOAP message. Because FreeIPA by default does not support use of biometric data for authentication, MMBio service was added to FreeIPA services, and authentication requests were diverted to it [25].

To implement such multifactor authentication, changes were made both on the server side and the client side of FreeIPA. For successful biometric authentication, it is necessary to map UserID used in FreeIPA solution to MMBioID used in MMBio framework. Each user in the identity management server has MMBioID attribute. This attribute uniquely identifies the user in the database of multi-modal biometric samples. On the client side, user authentication process needs to send one or more biometric samples in addition to password. Biometric samples will be the key for verifying the identity of person who submitted the password.

During the authentication process, on the client-side, PAM-aware applications need to be able to notify the user to provide a biometric sample in addition to password. Biometric authentication is only possible if there is a device connected to the computer and capable to obtain biometric sample. SSSD is responsible for communication between NSS/PAM components and PAM-aware applications. It needs to provide the following: [26]

- To handle authentication which requires multiple round trips between an SSSD client and one of its backend processes
- To enumerate the set of devices those are available on the system for obtaining biometric samples

SSSD client must pack the password and all of biometric samples sampled in one package (Fig. 2). Because biometric samples have sensitive nature, authentication package should be highly secured. In order to protect biometric samples, communication channel must be properly secured.

Inside a local area network, it is possible to physically secure communication channel, as access to network infrastructure can be controlled. On public networks, data can be only secured by encryption. In order to achieve this, two layers of encryption are used. At the first level, package is protected with HTTPS/TLS. However, TLS has some security risks [27]. Some of the threats described in [27], such as compression attacks and CSRF(Cross Site Request Forgery), are not applicable for our system, as they are based on web browser flaws. Other attacks, such as theft of RSA private keys, or bugs in TLS implementations are theoretically possible.

To mitigate this risk, we have added a second level of encryption. At second level, package is contained within an encrypted SOAP message[28]. Kerberos token is used for message encryption. Therefore, client machine has to be joined to identity management system. On every login, each user is provided with a Kerberos token. After that, user has to request a service token for MMBio service (Figure 2). After that, client sends his authentication request together with his service and client token.

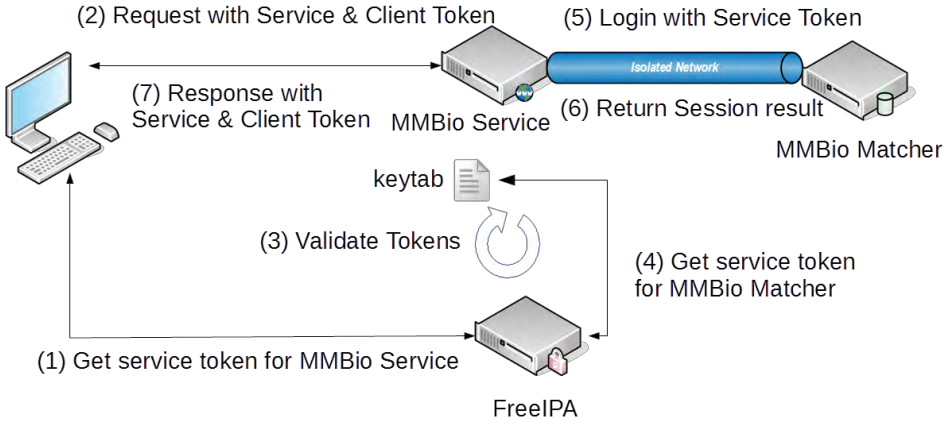

Fig. 2. System authentication workflow

MMBio service validates tokens according to server keytab configuration. MMBio service than acquires service token for MMBio matcher and logs in to MMBio matcher (Multimodal Biometric Matcher). After the response from matcher is received, the service will decide whether the authentication process has successfully conducted or not.Client gets service response with service and client token.

Therefore, client can be sure that he has received the answer form valid source. As second layer encryption (SOAP) contains hash values of encrypted data, even if TLS is breached, it is not possible to create a valid spoof message. For possible attacks to succeed, attacker would need to compromise client machine operating system.

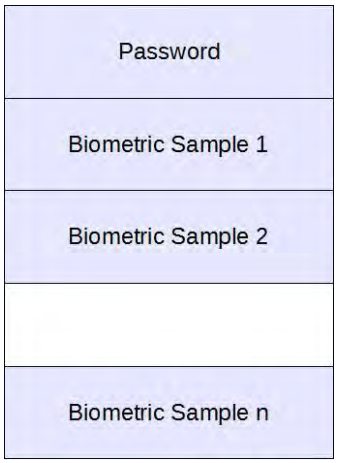

Fig. 3. Extended Packet for authentication

It is necessary to pair the identities stored in the FreeIPA server and the MMBio service, due to different ways of storing user information. MMBio service needs to know which identity from FreeIPA repository has biometric samples in its database and vice versa. In this way, communication between FreeIPA and MMBio service transmits

a minimum set of data sufficient to unambiguously determine the identity of a user during authentication process.

MMBio Matcher uses unique identifier MMBioID to determine identity of the user. The process of adding users in MMBio database is process of taking the biometric samples. Upon completion of the acquisition of samples it is necessary to bind MMBioID to the identity of a user in FreeIPA storage.

On the other hand, the process of adding a new identity in FreeIPA environment includes creating a user profile and binding it to an MMBioID. We have two scenarios:

- Newly created user does not have enrolled biometric samples in MMBio database,
- Newly created user is already enrolled in MMBio database

In the first scenario we need to take biometric samples from the user and upload them to the MMBio database. The second scenario is trivial. We need to bind the user identity with existing MMBioID.

7. Integrating Multimodal Biometrics into FreeIPA

A suggested technical solution is based on FreeIPA and MMBio solutions. Identity management is done with the help of FreeIPA system, while MMBio framework for multimodal biometrics is responsible for working with biometric data. A multimodal biometric application has been developed using framework.

In order to build a multimodal biometric system from unimodal open source solutions, several challenges have to be solved. It is necessary to establish communication between open source unimodal solutions, acquisition sensors, biometric database and multimodal fusion algorithms. Also, this communication has to be implemented in accordance with the system distributed nature, as different system components can be deployed on various platforms. Moreover, biometric data management has to be implemented, with special focus on supplying data in accordance with unimodal biometric solutions specifications.

MMBio framework for multimodal biometrics was developed to overcome these challenges. Communication between different system parts is based on MMBio communication protocol. Communication protocol is used rather than object serialization because communication protocols are platform independent. However, unimodal solutions and acquisition sensors often support only nonstandard, solution specific communication methods. In such situation, it is necessary to develop a communication adapter in order to translate protocol commands to solution specific ones.

MMBio framework supports different multimodal database work modes. It is possible to use either centralized or distributed database. Also, biometric data associated with an identity can significantly differ from one biometric system to another. In a multimodal biometric database, a person can have data about several different biometric modalities, and each modality may be represented by several data instances. Biometric data can be in raw form, or stored as biometric characteristics. Each type of biometric data can be stored in different file formats, and some file formats are solution specific.

MMBio communication protocol has been designed to comply with different biometric database models, and supports different use case scenarios.

System operates in verification mode. Biometric data and identity claimed by the user are sent to Multimodal biometric service – MMBio service. MMBio service finds according MMBioID for user in LDAP directory. Biometric data and MMBioID are sent to Multimodal biometric matcher (MMBio matcher), for each modality. Each unimodal solution compares biometric data to templates stored in multimodal biometric database. Calculated match scores are fused in fusion module, and final match score is returned to multimodal biometric server. Based on system threshold, user identity is verified or rejected.

8. MMBio Matcher (Multimodal Biometric Matcher)

Within the application, three different open source solutions have been integrated and each of them works with different biometric modality. The modalities used are: fingerprint, face and voice. For fingerprint NIST NBIS solution was used [29], for facial recognition an application developed using OpenCV [30], and voice application was based on MARF framework [31].

NBIS uses Bozorth[29] algorithm for matching templates, and Mindtct[29] utility for feature extraction. Algorithms are minutiae based, and are designed to be rotation and translation invariant. Bozorth constructs a compatibility table which consists of a list of compatibility association between two pairs of potentially corresponding minutiae. Match score represents length of longest path of linked compatibility associations.

MARF is open-source solution for text independent speaker recognition. It supports different feature extraction, normalization and matching algorithms [31]. In our system Fast Furrier Transformation were used for feature extraction, and Chebyshev distance for matching biometric characteristics.

For facial recognition an application developed with help of OpenCV framework was used. LDA[32] was used for face recognition, together with HAAR[32] cascades for face detection.

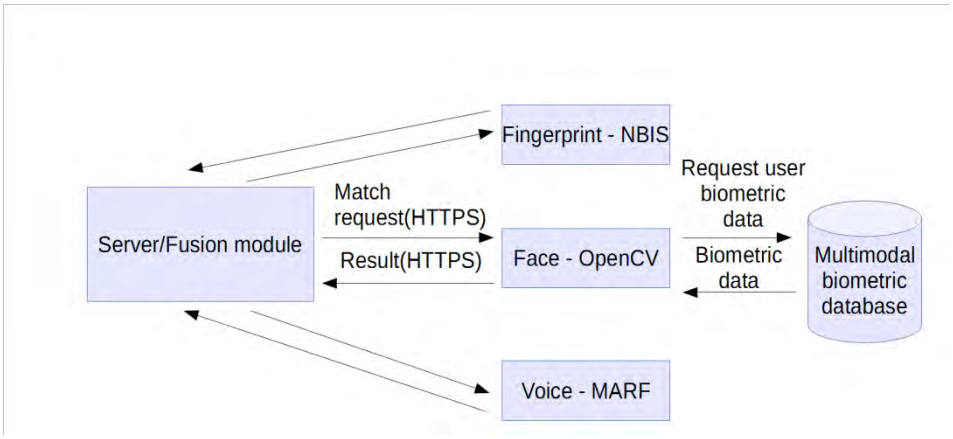

Fig. 4. MMBio matcher architecture

Although each of the open source solutions has lower accuracy than commercial solutions available on the market, when different modalities were combined, the accuracy of the system was at a higher level than it was with any unimodal solution individually [33].

Communication adapters are used for protocol message translation. Each component reports its functionalities to multimodal system during the initialization process. Communication between components is synchronized, based on request/response paradigm. In this use case, MMBio protocol is implemented by using REST (Representational State Transfer) services. Communication between multimodal server/fusion module and adapters for unimodal solutions is done over HTTPS protocol. Such approach allows communication between solutions deployed on different hardware platforms and operating systems. Adapters for unimodal solution communicate with the biometric database. Scalability is easily achieved, as each unimodal algorithm can be distributed on different hosts.

Server/Fusion module sends HTTPS request to each unimodal solution, and receives a HTTPS message containing a match score as a result. Example shows a biometric data match request which is being sent to a unimodal biometric solution. Header fields are used to describe request in detail. MMBioID, information about biometric modalities and sample types, content type are contained in the request header. Biometric-Sample-Type field describes whether biometric data is raw or processed. Payload contains extracted biometric characteristics that are to be verified. In the example, Jersey framework was used to implement REST web services. Communication between Server/Fusion module and unimodal solution adapters is performed on a isolated network. Only Server/Fusion module and unimodal solution adapters are allowed access to this network.

```
  POST /NBIS/resurs/match HTTPS/1.1Content-Type: image/jpeg
  User-Agent: Jersey/2.2 (HttpUrlConnection 1.7.0_25)
  Host: 10.10.1.176:8080
  Connection: keep-alive
  ServiceName: NBISFingerprint
  MMBioID: 1120
  Timestamp:09.09.2013. 14:54:03
  Modality:Fingerprint
  Biometric-Sub-Type: index finger
  Biometric-Sample-Type: raw image/bmp
  Content-Length: 277921

  PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+V
GhpcyBpcyB0aGUg
  Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+C
g==
  ..........................................................
..............
```

8.1. Score Normalization

Fusion module uses score level fusion. Before fusion, scores are normalized by one of the following algorithms [20]:

Min-Max. Score values are translated to domain with range of [0,1]

$$n = \frac{s-min(S)}{max(S)-min(S)} (1)$$

Z-score. Random variable S is standardized to normal distribution with parameters N(0,1)

$$n = \frac{s-mean(S)}{std(S)} (2)$$

Tanh. This method is considered robust to outlying values. Score values are translated to domain with range of [0,1]

$$n = \frac{1}{2}\left[\tanh\left(0.01\frac{s-mean(S)}{std(S)}\right)+1\right] (3)$$

8.2. Score Fusion

After normalization, match scores are fused by one of the algorithms described below. Finally, system compares fused score with preset threshold. In case of similarity metrics, if fused score is higher than preset threshold, claimed identity is verified.

Simple Sum.

$$f_i = \sum_{m=1}^{M} n_i^m, \forall i (4)$$

Matcher Weighting. Each score is given a weight factor, based on EER(Equal Error Rate) of unimodal solution

$$f_i = \sum_{m=1}^{M} \omega^m n_i^m, \forall i (5)$$

ω^m represents weighting score for unimodal biometric solution m, while r^m stands for unimodal solution EER

$$\omega^m = \frac{1/\sum_{m=1}^{M}\frac{1}{r^m}}{r^m} (6)$$

User Weighting. Each user is given custom weight factor for each modality, based on previous enrollments. Formula for calculating coefficients is given in detail in [20]

9. System Deployment and Applications

For evaluation and testing purposes, we have deployed server side of our system on three server machines. Used configurations contain Pentium 4 class processors running

on 3.0 Ghz and have 4GB RAM. Local area Ethernet network performs at speed of 1Gb/s. Clients machines for test are virtualized, and all are SSSD aware. All hardware used for configurations is common and affordable, including finger reader and camera.

Common part on each server is minimal Linux installation. On each server has been installed corresponding part of software packages. First server was used for identity management and it contains a FreeIPA server instance. It is configured with default settings. FreeIPA user scheme is extended with MMBioID attribute. MMBio matcher was deployed on separate server together with biometric database. Another server instance was the MMBio Service. It was added to the FreeIPA domain.

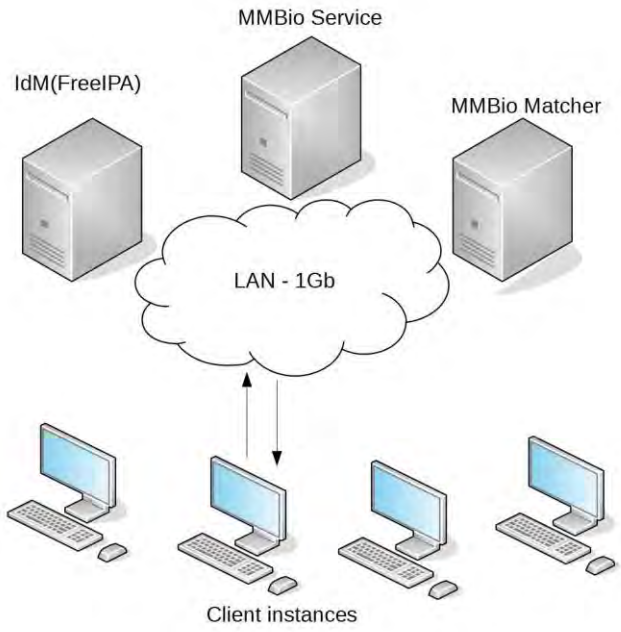

Fig. 5. System deployment

Every client is virtual machine with Desktop Linux installed on it. Also, each client is logged on FreeIPA domain. Clients have access to the biometric devices on the virtual host. During performance tests, a custom program was used to compose message for authentication with biometric samples.

There are various possible applications for such a system. Small and medium sized organizations with several applications and different user roles are possible candidates. Often cause for security breaches is human factor. People are sometimes careless with their passwords or authentication tokens. As biometric authentication represents something that user is, rather than something he knows or possesses, system security can be significantly improved. Such security improvement is especially important in organizations that work with sensitive data, such as finance and healthcare industries.

In addition to improved authentication security, users are granted SSO functionality for available applications or services. With other FreeIPA functionalities, this offers a solid foundation upon which various software systems can be developed.

10. System Evaluation

10.1. System Performance

To evaluate system performance, we have measured response time and CPU load on client instances. Each request represents a system verification attempt, using fingerprint, facial and voice biometric data. Relationship between number of parallel request and response time and CPU load is shown on Table 1.

We have estimated average weight of encrypted biometric data in request at about 500KB. As 1Gb represents 125 MB data, theoretically it would be possible to have about 250 parallel request in one second. A more realistic estimate should include other network traffic, and data reserved for protocol headers. Therefore, estimated number of request per second is somewhat lower than 250. However, current system bottleneck is MMBio matcher, as it is responsible for most of the total response time. Therefore, we can conclude that current network infrastructure leaves significant room for performance improvements.

Table 1. Deployed system performance

Number of parallel requests	Total Response time(ms)	MMBio matcher response time(ms)	MMBio matcher CPU load
1	583	501	7%
5	650	605	12%
10	1359	1310	20%
20	1949	1906	24%
30	2780	2702	40%
50	5286	5205	85%

10.2. System Precision

System precision has been tested on two datasets. First dataset was collected as a part of Multimodal biometry in identity management project. It contains biometric data of 39 subjects, 20 male and 19 female. Subject age varies from 25 to 65 years. For testing purposes facial, fingerprint and voice data were used.

Fingerprint data was collected by optical scanner. Samples were saved in 500x500 resolution with 8dpi pixel depth. Four right finger images of each person in the database were used in the testing. Also, four frontal facial images for each person were used. Pictures were saved in .bmp format, in 640x480 resolution. Voice data collected

was recorded in stereo mode with 44 kHz sampling rate. Speakers had to read short text and several random 4 digits codes.

After unimodal feature extraction and matching, 234 genuine and 741 imposter scores were generated, and subjected to normalization and fusion. Results are shown on Figure 5. ROC curves were used for results presentation. GAR stands for Genuine Acceptance Rate – percentage of genuine users successfully verified by the system, while FMR stands for False Match Rate – percentage of imposters successfully logged on to the system.

As expected, experiment results showed that NBIS unimodal fingerprint performance was the most precise among the unimodal solutions. However, combination of face, voice and fingerprint data lead to best system precision. Differences between different normalization and multimodal fusion methods were not significant on this dataset, most likely due to the small dataset size.

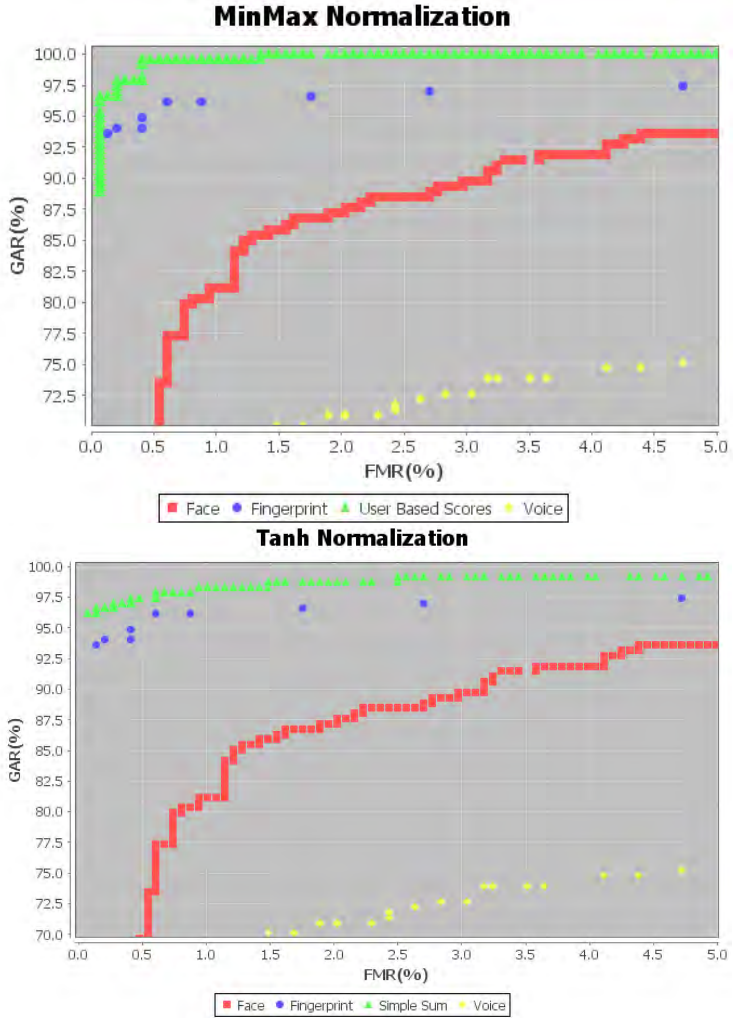

Fig. 6. System precision on dataset collected as a part of Multimodal biometry in identity management project

Second dataset used was an open access CASIA database [34]. We have constructed a chimeric [35] dataset from facial and fingerprint data. This dataset has a somewhat larger size, as it includes biometric data collected from 500 individuals.

CASIA database contains 2500 facial images collected from 500 subjects. Acquisition was performed with Logitech USB camera and saved in 640x480 resolution. All facial images were collected in a single session. Database contains 20000 fingerprint samples. Fingerprint acquisition was performed by URU4000 sensor. Fingerprint images were saved as 8bit bitmaps with 328x356 resolution.

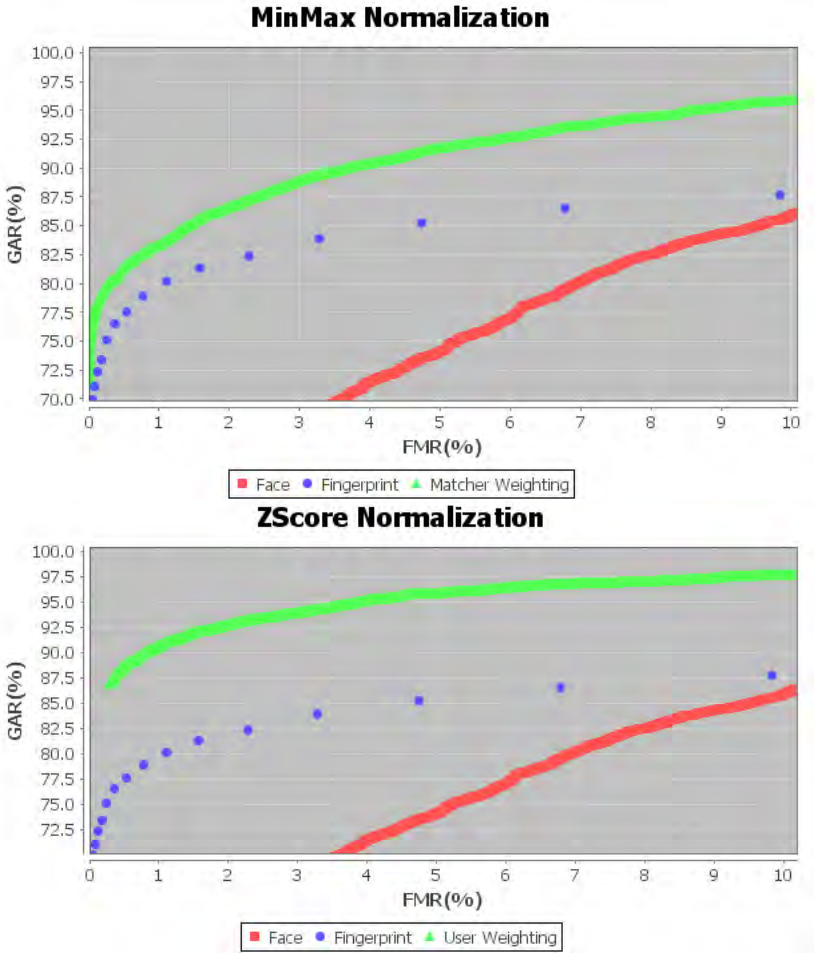

Fig. 7. System precision on CASIA dataset

Unimodal matching generated 3000 genuine and 124750 imposter scores. Fusion results are shown on Figure 6. Precision of unimodal solutions is significantly lower on this dataset. Due to outliers, the use Min-Max normalization method resulted in lower system precision. However, the use of multimodal biometrics has significantly improved system precision.

11. Conclusion

In this article a possible solution for strengthening user authentication is presented. Beside traditional user verification methods such as password, biometric authentication is also implemented. The goal was to implement biometric authentication in an identity management system by using open source solutions. As these solutions often have lower precision than their commercial contemplates, it was necessary to find a way to improve their performance. As multimodal biometrics improves overall system precision, several biometric modalities were used. Also, this approach allows us to utilize different combinations of hardware devices on client computers. For example, it is possible that on the client computer camera and microphone are available, but there is no fingerprint reader. In such case, it is still possible to perform biometric authentication by using available modalities.

SSSD was adapted to collect biometric data and store it in an authentication packet. Extended IdM with MMBio Matcher extracts biometric data and performs biometric recognition, and also verifies password in FreeIPA user repository. Such authentication scheme allows multifactor authentication. Also different repositories for user data can be used. An example would be possible use of Active Directory, which would allow us to authenticate users belonging to different domains.

Currently used unimodal solutions have displayed some precision deficiencies when working with large biometric datasets. In future, new algorithms and fusion schemes should be included. Also, as network throughput allows us to process more parallel requests than MMBio Matcher currently can handle, algorithm distribution scheme could significantly improve system performance. Also, the idea here is to bring algorithms were the data is, rather than to bring data to biometric solutions. In this way, both system speed and security can be improved.

For now, only traditional cryptographic methods have been applied for securing communication channels. As biometric data is irrevocable by nature, a possible use of revocable biometrics techniques will be topic for further research. Extracting biometric characteristics on client side, in order to improve performance and security, will also be considered.

Acknowledgement This work is a part of the project Multimodal biometry in identity management, funded by Ministry of Education and Science of Serbia, contract number TR-32013.

References

1. International Telecommunication Union: ICT Facts and Figures – The world in 2015. (2015). [Online].Availablehttp://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFacts Figures2015.pdf, (current July 2015)
2. European Commission. The Modinis IDM Study Team : Common Terminological Framework for Interoperable Electronic Identity Management. (2005). [Online] Availablehttp://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf (current July2015)
3. Lynch, L. : Inside the Identity Management Game, IEEE Internet Computing, vol 15. (2011)

4. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol 14. no.1 pp. 4-20. (2004)
5. Šošević, U., Milenković, I., Milovanović M., Minović M. : Support Platform for Learning about Multimodal Biometrics, Journal of Universal Computer Science 19, no. 11 pp. 1684-1700. (2013)
6. Milovanović, M., Minović, M., Starčević, D. : Interoperability Framework for Multimodal Biometry :Open Source in Action, Journal of Universal Computer Science 18, no. 11 pp. 1558-1575. (2012)
7. Jain, A.K., Nandakumar, K., Nagar, A. : Biometric Template Security, EURASIP Journal on Advances in Signal Processing, Volume 2008. 2008
8. Gillen, A., Waldman, B., Linux in the Mainstream: Growing Deployment of Business-Critical Workloads. IPC. 2011. [Online]. Available https://www.redhat.com/f/pdf/IDC_Linux_Mainstream.pdf (current November 2015)
9. Bertino, E., Martino, L., Paci, F., Squicciarini, A. : Security for Web Services and Service-Oriented Architectures, Springer-Verlag Berlin Heidelberg. (2010)
10. Kong, L., et all. : Identity Management White Paper - Draft, National Institute of Standards and Technology. (2011)
11. Al-Khouri, A.M. : PKI in Government Digital Identity Management Systems, European Journal of ePractice n° 15. (2011)
12. Sergio Sánchez, G., Oliva, A.G. :Is Europe Ready for a Pan-European Identity Management System?, IEEE Security & Privacy, vol 10. no. 4, pp. 44-49, (2012)
13. Williamson, G., Yip, D., Sharoni, I., Spaulding, K. : Identity Management: A Primer, MC Press, LLC. (2009)
14. Buecker, Bhatt, D., Craun, D., Ramanathan, J., Readshaw, N., Sampathkumar, G. : Integrated Identity and Access Management Architectural Patterns. (2008). [Online]Available: http://www.redbooks.ibm.com/redpapers/pdfs/redp4423.pdf(current July 2015)
15. RedHat Enterprise Linux, Identity Management Guide. (2013). [Online].Available:https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/index.html(currentJuly 2015)
16. FreeIPA: Identity/Policy Management. (2014). [Online]Available: http://www.freeipa.org/docs/master/html-desktop/index.html,(current July 2015)
17. Bogićević, M., Milenković, I., and Simić, D. : "Identity Management – A Survey" in Innovative Management and Firm Performance, M. Levi-Jakšić, S. Barjaktarević, M.Martić, Eds. Palgrave Macmillan, , ch. 19. (2014)
18. Ross, A., Nandakumar, K., and Jain, A.K. : Handbook of Multibiometrics (International Series on Biometrics). Springer-Verlag New York, Inc., Secaucus, NJ, USA. (2006)
19. Saini, N., Sinha, A., : Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction, Pattern Analysis and Applications. (2014)
20. Snelick, Robert; Uludag, U.; Mink, Alan; Indovina, M.; Jain, A., "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems," Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.27, no.3, pp.450,455. (2005)
21. Sim H., Asmuni, H., Hassan, R., Othman, R., : Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images, Expert Systems with Applications, Volume 41, Issue 11, 1, Pages 5390-5404, ISSN 0957-4174. (2014)
22. Monwar, M., Gavrilova, M.L. : "Multimodal Biometric System Using Rank-Level Fusion Approach," Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on , vol.39, no.4, pp.867-878 . (2009)
23. Monwar, M., Gavrilova M. : A Robust Authentication System Using Multiple Biometrics, Computer and Information Science Studies in Computational Intelligence , Volume 131, pp 189-201. (2008)
24. O'Gorman, L. : Comparing Passwords, Tokens, and Biometrics for User Authentication, Proceedings of the IEEE, vol 91, issue 12, pp 2021-2040. (2003).

25. Bogicevic M., Milenkovic, I., Simic D. : The Architecture of Integrated Identity Management and Multimodal Biometric System, XIV International Symposium Symorg, Serbia, Zlatibor, pp.900-907. (2014)
26. SSSD documentation, (2013) [Online]. Available: https://fedorahosted.org/sssd/wiki/DesignDocs(current July 2015)
27. Internet Engineering Task Force : Request for Comments: 7457 - Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS). (2015). [Online]. Available https://tools.ietf.org/html/rfc7457#section-2 (current November 2015)
28. PYSimpleSOAP library official webpage. [Online]. Available:https://code.google.com/p/pysimplesoap/(current July 2015)
29. Watson, C., Garris, M., Tabassi, E., Willson, C., McCabe, R., Jannet, S., Ko, K.: User's Guide to NIST Biometric Image Software, National Institute of Standards and Technology. (2010). [Online]. Available:http://fingerprint.nist.gov/NBIS(current July 2015)
30. Bradski, G. R., Kaehler, A.: Learning Opencv, 1st Edition (First ed.)., O'Reilly Media, Inc. (2008)
31. Mokhov, S. A. : Evolution of MARF and its NLP framework, In Proc. Third C* Conference on Computer Science and Software Engineering (C3S2E '10), ACM, New York, NY, USA. (2010)
32. Stan Z., Jain, A.K. : Handbook of Face Recognition, Springer-Verlag London. (2011)
33. Milenković, I., Pantović, V., Starčević, D., Minović, M. : "A multimodal biometrics system implemented using open source technology," Telecommunications Forum (TELFOR), 2011 19th Sep , pp.1352 – 1355. (2011)
34. Chinese Academy of Sciences, CASIA-FaceV5 biometric database. [Online]. Available http://biometrics.idealtest.org/(current July 2015)
35. Poh, N., Bengio, S.: Using Chimeric Users to Construct Fusion Classifiers in Biometric Authentication Tasks: An Investigation.2006 IEEE International Conference onAcoustics, Speech and Signal Processing. (2006)

Bojan Jovanović is a PhD candidate at University of Belgrade, Faculty of organizational sciences, Department for Information Technology. He currently works as a researcher at Laboratory for multimedia communications in Belgrade, Serbia. He published several research papers and participated in many research and commercial projects in Information Technology area. His interests include biometrics, computer security and system administration.

Ivan Milenković is a PhD candidate at University of Belgrade, Faculty of organizational sciences, Department for Information Technology. He currently works as a researcher at Laboratory for multimedia communications in Belgrade, Serbia. He published several research papers and participated in several research and commercial projects in Information Technology area. His interests include biometrics, computer security and mobile technologies.

Marija Bogićević is a PhD candidate at University of Belgrade, Faculty of organizational sciences, Department for Information Technology. She currently works as a researcher at Laboratory for multimedia communications in Belgrade, Serbia. She published several research papers and participated in several research projects in Information Technology area. Her interests include biometrics, identity management and e-commerce.

Dr Dejan Simić is a full professor at University of Belgrade, Faculty of organizational sciences, Department for Information Technology. He is engaged as a researcher at Laboratory for multimedia communications in Belgrade, Serbia. He published many research papers and participated in several research projects in Information Technology area. His interests include biometrics, computer security and e-commerce.

Received: October 30, 2014; Accepted: January 7, 2016