View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AIR Universita degli studi di Milano

Toward trust-based multi-modal user authentication on the Web: a fuzzy approach

Antonia Azzini
Università degli Studi di Milano
Dipartimento di Tecnologie dell'Informazione
via Bramante 65 26013 Crema (CR), Italy
azzini@dti.unimi.it

Stefania Marrara
Università degli Studi di Milano
Dipartimento di Tecnologie dell'Informazione
via Bramante 65 26013 Crema (CR), Italy
marrara@dti.unimi.it

***Abstract*— In the last few years authentication has become of paramount importance both on the corporate Intranets and on the global Web. While most approaches focus on the initial authentication and then no further check ensure the identity of the navigating user, in this work we present a fuzzy approach to multi-modal authentication for a trust-based, continuous identity check during Web navigation. The potentiality of such an approach for generating trust-based metadata is also discussed.**

I. Introduction

In the last few years, the web has entered the day-by-day life of million of people giving the opportunity to exchange lots of information by means of the interchange of documents. Recently the web community has asked for the possibility to integrate and combine data drawn from different sources, i.e., asking to navigate the web as an immense, integrated, data collection. Answer to this need is the *Semantic Web* [1], which includes a common format for integration and combination of data drawn from different sources, and a language for recording how the data relates to real world objects. Obviously, in such a powerful environment security plays an important role since it allows to insert data reserved to trusted users into this "integrated source". Hence, ensuring an adequate level of protection to data is an essential part of any comprehensive web security program, and often this means to provide a strong and effective access control system. While most researchers have focused on protecting data and documents (often expressed in XML) [3], we believe that the effectiveness of access control systems rests on one initial important assumption, proper user identification [4]: no one should be able to acquire the access rights of another person. In the literature [9] this condition has been faced with two different approaches: *biometric identification* and *biometric authentication*. Biometric identification and authentication are differentiated as follow: biometric identification occurs when an individual provides a sample biometric, sometimes without any additional knowledge, and the system must compare that sample with every stored record to identify a match. This is known as a one-to-many match, and is executed without any corroborating data. By contrast, biometric authentication occurs when an individual presents a biometric sample, and some additional identifying data, such as a photograph or password, which is then compared with the stored sample for that individual. Biometric authentication provides some inherent advantages as compared to other non-biometric identifiers since biometrics correspond to a direct evidence of the personal identity versus possession of secrets which can be potentially stolen. Moreover, most of the times the biometric enrollment is executed in-person and in controlled environments making it very reliable for future use. Both engines try to check the user's credentials before granting access to a computer system.

Some issues related to *strong* (i.e., biometric) authentication methods are still unsolved. In some cases, if the input sample quality is not sufficient for further processing, the system must reacquire data, and the resulting system might be more complicated or more expensive. Furthermore some biometric sensors, particularly those having contact with users, have a limited lifetime. In highly sensitive environments, such as health-care databases, it may be necessary to perform strong authentication many times (e.g., at random intervals) to prevent identity substitution after the initial authentication step. In such a scenario, the authentication system must distinguish between the initial step, in which it uses strong authentication to identify the user, and the following authentication steps in which the system decides if its trust in user's identity is high enough to allow the user to continue to perform the activity she is doing. *Multi-modal* biometric systems integrate multiple authentication techniques. Multi-modality will be important for many security applications, including checking the digital passports of the future, incorporating biometric data besides the portrait image. In this paper, we propose a multi-modal authentication system that combines strong authentication with conventional password-based techniques providing high accuracy. In our approach, different trust levels are set for different methods of authentication. When a user gains access to a protected part of the web, our system continuously checks whether the users' authentication data can be trusted, e.g. enough to satisfy the required security clearance level. In this way, users are kept under a continuous authentication process and security clearance levels can be rigorously maintained. In particular, focus of this paper is a deep discussion of the methodologies for biometric authentication available w.r.t. their possible use in conjunction with a fuzzy controller. The paper is organized as follows: Sect. II contains a brief overview of advantages and drawbacks of authentication

techniques, Sect. III discusses the basic problem posed by a fuzzy representation of biometric authentication techniques, in Sect. IV we present our fuzzy controller for multi-modal authentication, and finally, in Sect. V we draw our conclusion and present some future work.

A. Related Work

Several security methods for user authentication to control access to an information service have been discussed in the literature, showing how the identity theft becomes a critical issue, together with the management of rights. Indeed, as previously defined, traditional authentication systems may become inadequate since they do not identify a user as such.

As indicated in the work carried out by Bhargav-Spantzel and colleagues [9], the act of impersonating others identities by presenting stolen identifiers or proofs of identities has been receiving increasing attention because of its high financial and social costs. For this reason, the adoption of biometric authentication systems becomes an emerging approach to the problem of reducing such identity theft. The authors provided a two-phase authentication mechanism for federated indentity management systems, preserving the privacy with biometrics techniques.

Further improvements have been carried out in the last few years, increasing the awareness that multi-modal authentication (i.e., techniques more than one form of credential to identify a user) is generally stronger than any single-mode authentication method. In multi-modal systems "redundancy" is used to tolerate possible failures of authentication devices, including those due to users anomalies (e.g., eye diseases which may prevent iris recognition systems from capturing an appropriate image of the user's eye, or skin diseases which may prevent fingerprint acquisition). In this context, the multi-modal approach was originally introduced in order to alleviate the drawbacks of each individual technique. The work [14] presents a multi-biometric verification system that combines speaker verification, fingerprint verification with face identification. The authors use a fuzzy decision support system in order to take into account the external conditions that can affect verification performances. They show how the fusion of the three techniques reduces the error rates of 48% w.r.t. the speaker verification alone. Another interesting work is [15] that improves security by using *typing biometric* to reinforce password authentication mechanism. Also this methodology employs fuzzy logic to measure the user's typing biometrics. About face recognition, [17] presents a face template matching algorithm based on a 3D head model created from a single frontal face image. In this way the matching is robust across variations in pose, expression and illuminations conditions. This work was extended in [18] where authors describe a method for tracking a face on a video sequence, by recovering the full-motion and the expression deformation of the face using 3D expressive facial model. From some characteristic face points given on the first frame, an approximated 3D model of the face is re-constructed. Using a steepest descent image approach, the algorithm is able to extract simultaneously the parameters related to the face expression and to the 3D posture. Industrial researchers at Hitachi (`http://www.sdl.hitachi.co.jp`) developed a fully-fledged multi-modal system capable of choosing the "right" authentication technique depending on the required security clearance level. However, to the best of our knowledge [16] is the first paper where multi-modality is applied to the problem of checking continuously user identity during a working session to avoid malicious behavior such as identity substitution.

II. Advantages and Drawbacks of Authentication Techniques

User authentication is essential for reliable access control and rights management systems to determine a user authorization to access the content [4]. Different authentication techniques may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or database, environmental conditions, and other application specific parameters. Several works have been carried out in the literature by considering these features. In the work of O'Gorman [7] a detailed comparison of strong (biometric) and weak (traditional) authentication technologies has been carried out, discussing about the potential attacks against each technique and the main issues related to several applications. Sect. II-A II-B briefly point out their main advantages and drawbacks.

A. Traditional Authentication Techniques

As previously defined, the main advantage of traditional techniques is that they are easy to implement in a authentication system, but they cannot identify the user as such. In the Knowledge-based case, a password can be guessed or searched by an attacker and a long, random, changing password is difficult to remember. In the other case, with Token-based, a physical device can be lost, stolen, forgotten or disclosed. Moreover, considering the trustworthyness in distributed systems, other several aspects regarding these techniques have to be considered, as follows.

- Knowledge-based techniques, thanks to challenge-response password protocols, have proved robust against replay and transmission attacks. However, these techniques do not support compromise detection and do not offer much defense against repudiation.
- Token-based techniques provide for compromise detection and add protection against denial-of-service attacks. The two main shortcomings of token-based techniques are high cost, and vulnerability to theft. Token validation requires equipment whose cost is comparable to the one of (much more secure) biometric systems.

B. Biometric Authentication Techniques

These methods are inherently more reliable than password-based authentication, as they are less easily lent or stolen than others; furthermore they are extremely difficult to copy, share and distribute. For this reason, biometric systems provide a much stronger defense against repudiation.

The main issue in biometric authentication systems is performance, defined considering different factors, depending on critical issues in the data acquisition phase. Problems also include limited lifetime of particular biometrics, and possible violations of the user privacy.

The most commonly biometric technologies implemented are reported below:

- *Fingerprint* is based on matching numeric information of finger minutie. It is easy, fast of use and the hardware devices are low cost. It has considered the higher authentication form from the people, even if some problems can occur during acquisition phase, in particular in dusty and humid environments.
- *Hand Geometry* involves analyzing and measuring the shape of the hand. It offers a good balance of performance characteristics and is relatively easy of use, the accuracy can be very high, together with a satisfactory hardware technology. Drawbacks are related to the sensitivity to high lighting.
- *Iris* analyzes features found in the iris, uses a fairly conventional camera element and requires no close contact between the user and the reader. It is genetic aspects independent and not easily alterable. For these reasons it has the potential for higher than average template-matching performance, even though easy of use and system integration have not traditionally been strong points with iris scanning devices, being still considered as an intrusive system.
- *Face* analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. It is a no-invasive approach and it does not require contact between the user and the phisical device. The main problem of this technique regards its sensitivity to a high lighting and to the evolvable features of the face.
- *Retina* involves analyzing the layer of blood vessels situated at the back of the eye. As established technology, this technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate, but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if a user wears glasses or is concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can give satisfactory results.
- *Voice* Speaker, or voice, recognition, is a biometric modality that uses an individual's voice for recognition purposes. The seemingly easy implementation of speaker recognition systems contributes to the process's measure weakness — susceptibility to transmission channel and microphone variability and noise. Systems can face problems when end users have enrolled on a clean landline phone and attempt verification using a noisy cellular phone. The inability to control the factors effecting the input system can significantly decrease performance.
- *Signature* analyzes the way a user signs her name. Signing features such as speed and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not and the physical devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Anyway, signature is still an evolvable feature, with a low-level stable factor. For this reason relatively few significant signature applications have emerged compared with other biometric methodologies.

III. Fuzzy Representations of Biometric Authentication Techniques

In this section we discuss which authentication device commercially available can be used with a fuzzy controller. Commonly biometric devices base their final decision (authenticated/refused) on a matching between a stored template and a new biometric acquisition, obviously each technique implements a different matching function and not all outputs of these functions are suitable to work as input of a fuzzy controller. Moreover, biometric matching is probabilistic in nature, which implies that two samples of the same individual are never exactly the same. In detail:

- *Fingerprint* is based on matching numeric information of finger minutie. There are basically two techniques: *minutie-based* and *correlation-based*. The first technique finds minutie and builds a matrix containing minutie coordinates; the matching value is computed on the basis of a distance function between the template and the new acquisition matrices. Instead, the second technique maps minutie position w.r.t. a fixed point, then the matching value is computed on the basis of the number of corresponding points between the template and the new acquisition images. If the matching values exceed a given threshold the authentication succeeds.
- *Hand Geometry* involves analyzing and measuring the shape of the hand. This technique registers about 90 different hand features such as length, width, or finger thickness. These metrics define the feature vector of the user's hand. The matching value is computed by a vectorial distance function. Again, if this distance exceeds a given threshold the authentication succeeds.
- *Iris* analyzes features found in the iris using an image captured in controlled environments. Using a 2D Gabor wavelet filter [24], the technique maps the segments of the iris into *phasors* (vectors). Iris patters are described by an IrisCode [25] using phase information collected in the phasors. To perform the recognition, two IrisCodes are compared. The amount of difference between two IrisCodes — Hamming Distance (HD) — is used as a test of statistical independence between the template and the new acquisition IrisCodes.
- *Retina* As discussed above, iris recognition utilizes the iris muscle to perform verification. Retinal recognition

uses the unique pattern of blood vessels on an individuals retina.

- *Face* analyzes facial characteristics. There are two predominant approaches to the face recognition problem: *biometric* (feature based) and *photometric* (view based). Many different algorithms were developed but the main three ones are: *Principal Components Analysis* (PCA), *Linear Discriminant Analysis* (LDA), and *Elastic Bunch Graph Matching* (EBGM). The PCA approach decomposes the face structure into orthogonal components known as *eigenfaces*. Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in 1D array. A probe image is compared against the template by measuring the distance between their respective feature vector. LDA is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. EBGM relies on the concept that real face images have many non linear characteristics that are not addressed by the linear analysis methods discussed earlier, such as variations in illumination, pose, and expression. A Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid. The *Gabor jet* is a node on the elastic grid, notated by circles on the image below, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing [1]. Precognition is based on the similarity of the Gabor filter response at each Gabor node.

  The most commercially used technique is the PCA, which is also the best suitable to join a fuzzy controller, just defining membership functions for the vector distance.
- *Voice* Speaker, or voice recognition, is a biometric modality that uses an individual's voice for recognition purposes [2]. The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual. A popular choice for remote authentication due to the availability of devices for collecting speech samples and its ease of integration, speaker recognition is different from some other biometric methods in that speech samples are captured dynamically or over a period of time, such as a few seconds. Analysis occurs on a model in which changes over time are monitored, which is similar to other behavioral biometrics such as dynamic signature, gait, and keystroke recognition. There are two forms of speaker recognition: *text dependent* and *text independent*. In systems using text dependent speech, the individual presents header a fixed (password) or prompted (please say 3 4 6 9) phrase that is programmed into the system and can improve performance expecially with cooperative users. Speech samples are waveforms with the time on the horizontal axes and the loudness on the vertical access. The speaker recognition system analyzes the frequency content of the speech and compares characteristics such as the quality, duration, intensity dynamics, and pitch of the signal. In text dependent system the voice sample is converted from an analog format to a digital format, the feature of the individual's voice are extracted, and then a model is created. Most test dependent speaker verification systems use the context of Hidden Markov Models (HMMs), random based models that provide a statistical representation of the sounds produced by the individual. The HMM represents the underline variations and temporal changes over time found in the speech states using the quality-duration-intensity dynamics-pitch characteristics mentioned above. Another method is the Gaussian Mixture Model, a state-mapping model closely related to HMM, that is often used for unconstraint text independent application. Like HMM, this method uses the voice to create a number of vector *states* representing the various sound forms, which are characteristics of physiology and behavior of the individual. These methods all compare the similarities and differences between the input voice and the stored voice states to produce a recognition decision. The input voice sample and enrolled models are compared to produce a *likelihood ratio* indicating the likelihood that the input sample came from the claimed or hypothesized speaker.
- *Signature* dynamic signature recognition uses multiple characteristics in the analysis of an individual's handwriting. These characteristics vary in use and importance from vendor to vendor and are collected using contact sensitive technologies, such as PDAs, digitizing tablets. Most of the features used are dynamic characteristics rather than static and geometric characteristics, although some vendors also include these characteristics in their analysis. Common dynamic characteristics include velocity, acceleration, timing, pressure, and direction of the signature strokes, all analyzed in the X, Y and Z direction. Some dynamic signature recognition algorithms incorporate a learning function to account for the natural changes or drift that occur in an individual's signature over time.

  The recognition methods vary widely. The dominant methods are feature analysis and stroke code sequences used by most of the commercial systems. Some systems use chain codes, some others use template matching or elastic matching. The chain codes are of extreme points: left, right, top and bottom. Template matching simply means matching an unknown character against stored

[1] A convolution expresses the amount of overlap from functions, blanding the functions together.

[2] It is a different technology than *speech recognition*, which recognizes words as they are articulated, which is not a biometric.

character templates. This template matching system matches sequences of x/y coordinates, probably in a linear manner. Elastic matching is a form of nonlinear template matching [19].

Obviously, not all the techniques presented above are suitable inputs for a fuzzy controller. For example fingerprint, hand geometry, iris, retina and face recognition base their matching function on the definition of distance values between templates and new enrollments, giving a straightforward definition of possible membership functions in a fuzzy controller. On the other side, behavioral techniques such as voice or signature authentication base their matching mechanism on statistical considerations making more difficult a possible interpretation in a fuzzy system.

Since our approach needs to continuously check the identity of the user while she is working, we want it to be the least intrusive as possible. Hence we will not consider devices such as retina or iris systems, because they would require the user to interrupt her activity for a while during the biometric acquisition process. In this work, we will not deal with fingerprint and hand geometry because these techniques require devices having a limited lifetime. More importantly, they hardly guarantee that the person who is provides biometric data is the same that was authenticated originally. For example, suppose that university students sit their exams using a computer application without faculty supervision. In such a scenario, identity substitution could easily be performed after authentication, with the consent of the authenticated user, even if the authentication system keeps on requesting fingerprints. The original user could just stay available to provide fingerprints when required, while another student works on the examination paper. On the other hand, in the case of face recognition a digital camera can be installed on the top of the computer display, pointing in the direction of the user. The user does not know if the entire session is recorded or if the camera is used only for an automatic authentication, therefore malicious behavior is less likely. Of course, face recognition suffers of other drawbacks such as inconsistent presentation (i.e. different acquisitions may represent different poses of a face), irreproducible presentation (e.g. due to facial hair growth, a broken nose or wearing eyeglasses) and imperfect signal/representation acquisition (e.g. due to different illuminations). However it has been experimentally tested [7] that face recognition is affected by a experimentally determined FNMR (False NonMatch Rate) of 16% and a FMR (False Match Rate) $= 16\%$. In our context these values can be decidedly reduced just by asking the user to check the illumination conditions of the room where she is working. However, face recognition is the choice we made in this setting and with the motivation stated above, but our approach is general enough to allow to choose one or more different biometric techniques to authenticate users in a different situation.

IV. A Fuzzy Controller for Multi-modal Authentication

In this paper, we propose a multi-modal authentication system that combines strong authentication techniques with conventional password-based techniques providing high accuracy. In our approach, for which we have presented a possible implementation with one biometric technique (face recognition) and a password based technique in [2], different trust levels are set for different methods of authentication. When a user gains access to a protected facility, our system continuously checks whether the users' authentication data can be trusted, e.g. enough to satisfy the required security clearance level. If trust is sufficiently high, no action is taken. When trust gets too low, the system chooses a suitable authentication technique, gets the corresponding biometric data, and decides whether the new information satisfies the required security level. In this way, users are kept under a continuous authentication process and security clearance levels can be rigorously maintained.

A. Architecture

Our approach includes a trust evaluation process which continuously checks the identity of the user who is performing a certain activity on the web. Figure 1 shows the basic steps of our process: after an initial authentication, the server can require further authentication steps based on two parameters 1) the level of trust previously computed and 2) the time passed from the last authentication. We suppose the first authentication to have been performed using both strong and weak techniques. Indeed the userID is used to choose in the database the template to be used in the matching of the biometric acquisitions, because in a matching one-to-one the error rates are significantly reduced. The following steps, instead, can be acquired by strong or weak techniques on the basis of the trust level.

B. Trust Evaluation Parameters

In our model each user authentication can be performed using strong or weak authentication techniques. The *BIO* value represents how the biometric enrollment matches the user's template, normalized in the range $[0, 1]$. The second authentication parameter, *TOK*, corresponds to the boolean output (low/high) of the weak authentication system which supports the evaluation of the trust in the user's identity during the activity. In our prototype we used a UserId/password system. At the initial authentication step, the weak technique is involved to enforce the biometric acquisition and the parameter *TOK*, if the authentication successes, is set to *high*, i.e. equal to 1. Two *aging* parameters, respectively for the biometric and the token parameter values, are defined in order to measure how the system's trust in the identity of the user decays in time [2].

1) Trust Evaluation Parameter BIO in case of biometric multi-modal authentication: In particular environments, where security is a strategic issue, it can be important to use a multi-modal technique for the evaluation of the parameter

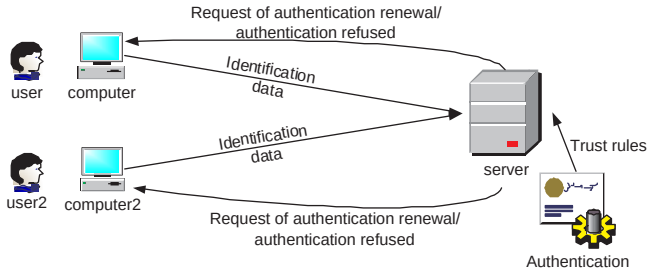

Fig. 1. Context for trust evaluation model.

BIO to be fed into the fuzzy controller. In literature there have been proposed many general strategies to combine multiple biometric classifiers. Among them, Ross and Jain [20] have proved that the SUM works well in improving significantly authentication performances w.r.t. a mono-modal approach. Other solutions include majority vote [21], optimal combination of patter classifiers [22], a weighted vote based on Dempster-Shafer evidence theory [23], binary operators, etc. Moreover, there are multiple factors that have to be considered when building a biometric multi-modal system:

- choice and number of biometric features;
- detail level in which feature information have to be integrated into the classifier;
- adopted methodology used to integrate information;
- cost versus performance evaluation analysis.

The evaluation of these factors strongly depends from the application and from the set of biometric techniques adopted. We defer a study in depth of these aspects of the problem to a future development of a case study with multi-modal biometric access.

C. Fuzzy Controller Operation

The entire process implemented in our approach is shown in Figure 2.

At the first step, the information obtained by the biometric engine, i.e. the value *BIO*, and the parameter *TOK* are fed into a fuzzy inference engine *Fuzzy Trust Model* in order to calculate a trust value *TRUST* that expresses the level of trust of the system in the user's identity after the initial authentication at time t_0. Of course, prior to processing of the inputs, it is necessary to define fuzzy membership functions which define the degree of membership of each input parameter in the context of the proposed model. Also, it is necessary to define the controller's fuzzy rules. These aspects strongly depend on the application and have been detailing discussed in [2] in case study that uses the face recognition authentication technique.

At time t_0 *BIO* and *TOK* are initialized; at each time t_i ($i > 0$), the decay rate of these values will depend on the corresponding aging parameters. The *TRUST* value is then defuzzified through a *Defuzzifier* engine, using the standard centroid-of-area technique. The output is then fed to another fuzzy engine, *Fuzzy DSS Model*, to compute the final level of trust. This second engine takes as inputs, together with the trust defuzzified value, also external conditions, that may become useful in such a multi-modal authentication approach, that consider biometric authentication techniques. Acceptance rate may degrade due to *context variables* (e.g., when the lighting is too bright or too dark). In this setting, these context variables are generally named *CONTEXT* and supposed, for simplicity, with possible fuzzy values "good" and "poor". The resulting trust of the Fuzzy DSS Model is defuzzified again with the standard centroid-of-area technique, and the output value is compared with the threshold of the membership functions of the Fuzzy DSS Model at each time t_i.

If the output trust is *low* the system asks for trust enforcement by going through the *Matching* phase. In this case the system asks for a user re-authentication, that can be biometric or knowledge-based, depending on the *BIO* and *TOK* values at that time t_i. In particular, the system re-acquires the parameter whose value at time t_i is less than a corresponding minimum threshold, previously defined, while maintains the same value at time t_i if it is more than the corresponding threshold. If the trust output is considered *medium* or *high* the system checks, through the *Time Controller* module, how the trust acquired at time t_i has been affected by the decay rate of the *BIO* and *TOK*, giving the new, decreased, parameter values for *BIO* and *TOK* at time t_{i+1}. These values are fed into the *Fuzzy Trust Model* in order to obtain the new trust value at time t_{i+1}.

When the trust level decays to the value of *very low*, the user inserts two wrong passwords in the same weak authentication step, or when the maximum value of the examination time is reached, the execution step goes to the *Close User Working Session* and the process stops.

Each of the two fuzzy models has been implemented (see [2]) with different rules, in order to control the trust value at each time step t_i with respect to different evolved parameters of *BIO* and *TOK*.

V. Conclusions

This paper focuses on the problem of a secure strong authentication of a web navigator. Our approach uses a fuzzy controller to continuously check the user identity during a working session. In this paper we deeply discuss biometric techniques characteristics and their possible use in conjunction with a fuzzy controller. Moreover we provide a draft of using our approach with a multi-modal biometric technique

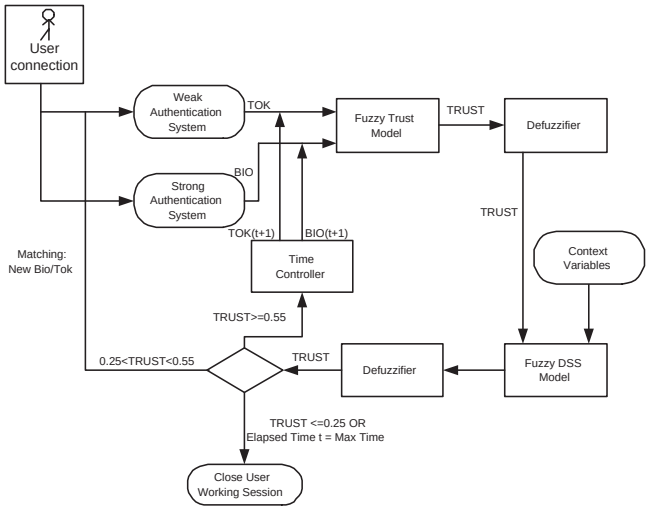

Fig. 2. Architecture of the Multi-modal Fuzzy Trust Model.

to compute the biometric input of the fuzzy controller. In the next future we plan to apply our solution to a real case using multiple devices to compute the biometric input, providing experimental results and performance analysis.

ACKNOWLEDGMENT

The authors thanks Ernesto Damiani for his evaluable comments on this work.

This work was partly funded by the Italian Ministry of Research Fund for Basic Research (FIRB) under projects RBAU01CLNB_001 "Knowledge Management for the Web Infrastructure" (KIWI). and RBNE01JRK8_003 "Metodologie Agili per la Produzione del Software" (MAPS).

REFERENCES

[1] Tim Berners-Lee, James Hendler and Ora Lassila. *The Semantic Web.* Scientific American, May 2001.

[2] A. Azzini, E. Damiani, and S. Marrara, *Ensuring the identity of a user in time: a multi-modal fuzzy approach*, International Conference CISDA 2007, 1-5 April 2007, Honolulu, Hawaii.

[3] Li Qin and Vijayalakshmi Atluri, *Concept-level Access Control for the Semantic Web*, Proceedings of the ACM Workshop on XML Security, October 2003.

[4] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, *Biometric Cryptosystems: issues and challenges*, Proceedings of the IEEE, vol. 92, num. 6, 948-960, June 2004

[5] C. Braz and J. Robert *Security and Usability: The Case of the User Authentication Methods* Proceedings of IHM 2006, 18th-21st April 2006, Montreal, Quebec.

[6] W.G. de Ru and J.H.P. Eloff *Enhanced Password Authentication through Fuzzy Logic*

[7] L. O'Gorman *Comparing Passwords, Tokens, and Biometrics for User Authentication.* Proceedings of the IEEE, vol. 91, no.12, 2021-2032, December 2003.

[8] E.H. Mamdani and S. Assilian. *An experiment in linguistic syntesis with a fuzzy logic controller.* International Journal Man-Machine Studies, 7:1-13,1975.

[9] A. Bhargav-Spantzel, A. Squicciarini and E. Bertino. *Privacy Preserving Milti-Factor Authentication with Biometrics*, Proceedings of the second ACM Workshop on Digital identity management DIM '06, November 2006.

[10] T. Takagi and M. Sugeno. *Fuzzy identification of systems and its applications to modeling and control.* IEEE Transactions on Systems, Man, and Cybernetics, 15:116-132,1985.

[11] G.J. Klir and B. Yuan. *Fuzzy Sets and Fuzzy Logic: Theory and Applications* Prentice Hall, Upper Saddle River, NJ, 1995.

[12] S. Schmidt, R. Steele and T. Dillon *Towards Usage Policies for Fuzzy Inference Methodologies for Trust and QoS Assessment* Proceedings of Fuzzy Days 2006, Dortmund, Germany, September 2006.

[13] S. Krawczyk and A.K. Jain. *Securing Electronic Medical Records Using Biometric Authentication* Proceedings of AVBPA 2005, ed. Springer, pp.1110-1119.

[14] C.W. Lau, B. Ma, H. M. Meng, Y. S. Moon and Y. Yam *Fuzzy Logic Decision Fusion in a Multimodal Biometric System* Proceedings of the 8th International Conference on Spoken Languages Processing (ICSLP) Korea, October 2004.

[15] W. G. de Ru and J. H. P. Eloff. *Enhanced Password Authentication through Fuzzy Logic.* Journal of IEEE Expert Intelligent Systems & Their Applications, November/December 1997.

[16] Antonia Azzini and Stefania Marrara, *A Fuzzy Trust model proposal to ensure the identity of a user in time.* Proceedings of Fuzzy Days 2006, Dortmund, Germany, September 2006.

[17] M. Anisetti, V. Bellandi, E. Damiani and F. Beverina. *Facial identification problem: A tracking based approach.* Proceedings of the 1st International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2005, November 27 - December 1, 2005, Yaounde, Cameroon, pp. 28-35.

[18] M. Anisetti, V. Bellandi, E. Damiani and F. Beverina. *3D Expressive Face Model-based Tracking Algorithm.* Proceedings of the IASTED International Conference on Signal Processing, Pattern Recognition, and Applications, SPPRA 2006, February 15-17, 2006, Innsbruck, Austria, pp.111-116.

[19] C.C. Tappert, C.Y. Suen, and T. Wakahara. *The State of the Art in On-Line Handwriting Recognition.* IEEE Transactins on Pattern Analysis and Machine Intelligence, Vol. 12, no. 8, August 1990.

[20] A. Ross and A.K. Jain. *Information fusion in biometrics.* Patter Recognition Letters, Vol. 24, pp.2115-2125, September 2003.

[21] Y.A. Zuev and S.K. Ivanov. *The voting as a way to increase the decision reliability.* Proceedings of Foundations of Information/Decision Fusion with Applications to Engineering Problems, Washington, DC, Aug. 1996, pp. 206-210.

[22] L. Lam and C.Y. Suen. *Optimal combination of pattern classifiers.* Pattern Recognition Letters, Vol. 16 , no. 9, pp.945-954, September 1995.

[23] L. Xu, A. Krzyzak and C. Suen. *Method of combining multiple classifiers and their applications to handwriting recognition.* IEEE Transactions on Systems, Man and Cyernetics, Vol. 22, no.3, pp.418-435, May/June 1992.

[24] X. Wu and B. Bhanu. *Gabor wavelet representation for 3-D object recognition.* IEEE Transactions on Image Processing, Vol.6, no.1, pp.47-64, January 1997.

[25] J.G. Daugman. *High Confidence Visual Recognition of Persons by a Test of Statistical Independence.* IEEE Transactions on Pattern Analysis

and Machine Intelligence, Vol. 15, no. 11, pp. 1148-1161, November 1993.