A Pervasive Biometric Identification Services Platform using Support Vector Machines

Juan Miguel Gómez, Maria Jesús Poza, Belén Ruiz Mezcua, Luis Puente
Universidad Carlos III de Madrid
Avda de la Universidad, 30, Leganés, Madrid, Spain
{juanmiguel.gomez, maria.jesus, belen.ruiz, luis.puente}@uc3m.es

ABSTRACT

Services have reached a new access dimension in a Ubiquitous Computing and pervasive Internet environment. Enabling Pervasive Services to provide value-added functionality as well as designing them for a convenient and trusted usage has become a major concern. Biometric Identification usually refers to identifying an individual based on his or her distinguishing traits. This paper presents an architecture to enable Biometric Identification through a Pervasive Services Platform to enable restricted access, based on the identity of the user. The focus of the research is on using Support Vector Machines (SVMs) on enabling user access through appropriate authentication mechanisms. Depending on the security requirements of the user, Internet trust mechanisms or mobile-based key exchange mechanisms can be applied. The user-centric approach will enable the user to select an identity provider for trusted management. A proof-of-concept prototype in the context of the PIBES project is also presented.

Keywords: Biometrics, Gaussian Mixture Models, Pervasive Services, Support Vector Machines, Ubiquitous Computing.

1 INTRODUCTION

Pervasive Services are shifting the paradigm of Ubiquitous Computing towards value-adding strategies. Rapid service access and Internet services are currently a commonality. The majority of customers use computers for this type of service access, appreciating the convenience of a good user interface. However, computers have a number of disadvantages, they suffer from 1) the insecure computer environment and infrastructure and 2) the limitations of certain environments. While insecure computer environments and infrastructure are the subject of research in various projects, the limitations of a quasi-stationary environment, at work, at home or in the office is a hinder for active participation in social communities [Noll, 07]. According to a study from the Ball State University, average PC usage is just above 2 h/day [Ball et al, 06]. This limits the access of PC-based users to such knowledge intensive services and most of the potential users currently work to establish a mobile portal to their communities.

Biometric Identification usually refers to identifying an individual based on his or her distinguishing traits. In principle, a biometric identity is based on the premise that a measurable physical or behavioral trait is a more reliable indicator of identity than the traditional systems such as pairs composed by password and username, Personal identification numbers (PIN) and the like. Particularly, since biometric identity technologies deal with security and privacy issues, the challenge for the research community is to attain integrated solutions that provide an entire solution, from sensors and data acquisition to biometric data analysis and system design.

In this paper, we present a fully-fledged Pervasive Services Platform which provides ubiquitous Biometric Identification, ensuring privacy and security. We use Support Vector Machines (SVM) as a set of related supervised learning methods used for classification and regression.

The remainder of this paper is organized as follows. In Section 2, we introduce the problem statement and motivating scenario for our Pervasive Services platform, the gist of our work, the Pervasive Service Platform and the use of SVMs. Section 3 presents the results and proof-of-concept implementation based in a real world scenario in the PIBES project. Finally, conclusions and related work are discussed in Section 5.

2 A PERVASIVE BIOMETRIC IDENTIFICATION SERVICE PLATFORM

New methodologies, techniques and tools are necessary to develop and maintain Pervasive Services for the future. However, current technologies such as Service Oriented Architectures (SOA) and Web Services (WS) have gradually advanced to show their viability, especially if they are used in combination. Semantic Technologies and SOA technologies are widely acknowledged to play an important role in solving the interoperability problem between applications; the usage of semantic description in the context of advanced services delivery is expected to support easy access to the services. Such formal and explicit descriptions not only enable easy service integration, but will also support exchange of preferences, profiles and context information of mobile users. In our work, we provide an extension of simple Pervasive Web Services with Biometric Identification and policies, representing security requirements for service discovery and privacy protection of user requests. This paper suggests extending the usage of biometric identification and recognition to user preferences and context, thus it allows extraction of only the required information for a specific service request.

2.1 Conceptual Model

Pervasive Mobile Services have moved to a Web service oriented architecture. In [Noll, 06b] semantic annotation of advanced Telecom services was used to achieve exchange of roaming information on a dynamic basis. The main findings of the approach were the cost reductions in service delivery, due to reduced effort for testing and updating of Web services in a semantic service world.

2.2 Support Vector Machines (SVMs)

SVM (Support Vector Machine) is a useful technique for data classification. It is described in [Burges, 98]. A classification task usually involves training and testing data which consist of some data instances. Each instance in the training set contains one "target value" (class labels) and several "attributes" (features). The goal of SVM is to produce a model which predicts target values of data instances in the testing set which are given only the attributes.

Given a training set of instance-label pairs (x_i, y_i), i = 1, . . . , l where $x_i \in Rn$ and $y \in \{1,-1\}^l$, the support vector machines (SVM) require the solution of the following optimization problem [Boser, 92], [Cortes, 95].

$$\min_{\mathbf{w},b,\xi} \quad \frac{1}{2}\mathbf{w}^T\mathbf{w} + C\sum_{i=1}^{l}\xi_i$$

$$\text{subject to} \quad y_i(\mathbf{w}^T\phi(\mathbf{x}_i)+b) \geq 1-\xi_i,$$

$$\xi_i \geq 0.$$

Here training vectors x_i are mapped into a higher (maybe infinite) dimensional space by the function ϕ. Then SVM finds a linear separating hyperplane with the maximal margin in this higher dimensional space. C > 0 is the penalty parameter of the error term. Furthermore, $K(x_i, x_j) \equiv \phi(x_i)^T \phi(x_j)$ is called the kernel function. Though new kernels are being proposed by researchers, the following four basic kernels are used:

- Linear: $K(x_i, x_j) = x^T_i x_j$.
- Polynomial: $K(x_i, x_j) = (\gamma x_i^T x_j + r)^d$, $\gamma > 0$.
- Radial basis function (RBF): $K(x_i, x_j) = \exp(-\gamma\|xi - xj\|^2)$, $\gamma > 0$.
- Sigmoid: $K(x_i, x_j) = \tanh(\gamma x_i^T x_j + r)$.

Here, γ, r, and d are kernel parameters.
In our software, the Kernel function used is the RBF function.

3.2.1 GMM Vs SVM

The two most popular techniques in pattern recognition are discriminative classifiers and generative model classifiers: GMM and SVM. The performance of both methods appears very similar according to previous research, however, combining them together could improve the performance of the recognition system [Dong, 01]. This possibility could be explored in future studies.

2.3 Biometric identification based on voice recognition

The verification of the speaker involves determining whether the claimed identity of the speaker corresponds to the true identity of the speaker, through biometric identification based on features extracted from the speaker's voice.

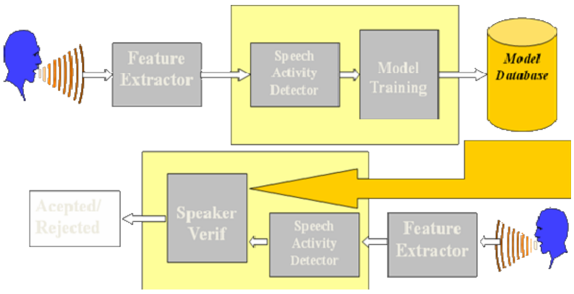

Figure 1. Diagram of the stages of biometric identification based on voice recognition.

Anatomical variations that naturally occur amongst different people and the differences in their learned speaking habits manifest themselves as differences in the acoustic properties of the speech signal. By analyzing and identifying these differences, it is possible to discriminate among speakers. Our front end of the speech module aims to extract the user dependent information.

2.4 Architecture

The verification module consists of two stages: (1) the training stage and (2) the operational stage. At training phase, several sample utterances from each system user are collected in order to get a ‘speech model’ from each user. At the operational stage, we opted for two emerging classification algorithms: GMMs and Support Vector Machines (SVM) to compute the distance between the subject trained model and the input sample. We wish to assess the performance of both algorithms to determine with which we can most accurately perform speaker recognition.

The system includes three important stages: endpoint detection, feature extraction and pattern generation/comparison. The endpoint detection stage aims to remove silent parts from the raw audio signal, as this part does not convey speaker dependent information.

The feature extractor is MDCC based, as for speech/speaker recognition, the most commonly used acoustic feature are mel-scale frequency cepstral coefficient (MFCC for short) [Paliwal, 05], [Jang, 07]. We use Pre-emphasis (0.97), Frame blocking (The length of the speech window is 25 milliseconds, the period is 10 milliseconds), Hamming windowing, FFT, Triangular Bandpass Filters (26 filters), Using the Discrete cosine transform we calculate 12 cepstrum for each voice sample frame and the logarithm of the energy level. For each of these 13 parameters we evaluate its speed coeficient and therefore we get a 26 feature vector for each sample frame. We calculate the mean value for each feature along the set of vectors from a full speech and then we substract it again from the features in every vector. And finally we normalize the energy level by dividing this feature by its absolute maximum value. So, we use a feature vector with 26 coefficients.

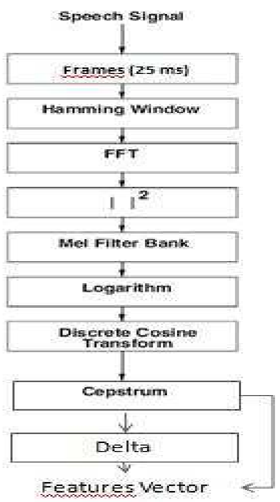

Figure 2. Feature extractor modules.

3 RESULTS

The two above-mentioned algorithms were tested in three different noise environments: “controlled” environment (low noise level), “graded” environment (medium noise level), and “adverse” environment, with a high level of noise, and masculine/feminine at 50% (based on the biometric database BANCA). The current results of our research are shown in the table below:

	FA	FR	HTER
Controlled environment, Group 1	1%	0%	0.48%
Controlled environment, Group 2	0%	0%	0%
Controlled environment: average	0.5%	0%	0.24%
Graded environment, Group 1	0%	2.6%	1.28%
Graded environment, Group 2	1%	1.3%	1.12%
Graded environment: average	0.5%	1.95%	1.2%
Adverse environment, Group 1	3.8%	3.8%	3.8%
Adverse environment, Group 2	6.7%	3.8%	5.29%
Adverse environment: average	5.25%	3.8%	4.55%

Table 1. Results with GMM algorithm

Sex	P_FR	P_FA	Pe
Masculine	0%	3.84%	1.92%
Feminine	0%	11.53%	5.77%
Total	0%	7.69%	3.84%

Table 2. Results with SVM: Controlled environment

Sex	P_FR	P_FA	Pe
Masculine	0%	3.85%	1.92%
Feminine	0%	15.38%	7.69%
Total	0%	9.61%	4.81%

Table 3. Results with SVM: Graded environment

Sex	P_FR	P_FA	Pe
Masculine	3.85%	7.69%	5.77%
Feminine	0%	34.61%	17.31%
Total	1.92%	21.15%	11.54%

Table 4. Results with SVM: Adverse environment

5 CONCLUSIONS AND FUTURE DIRECTIONS

Even though previous research has stated that the comparison of the classification algorithms GMM and SVM did not demonstrate significant differences in performance [Lalonde, 07], and [Adams, 03] claims that SVM outperforms GMM, our results indicate that it is possible to improve the results of the SVM classification algorithm; this is the subject of our current research.

6 REFERENCES

[Adams, 03] Adams, W.H. et al. 2003. *Semantic Indexing of Multimedia Content Using Visual, Audio, and Text Cues*. EURASIP Journal on Applied Signal Processing, 2, pp. 170–185.

[Boser, 92] Boser, B., Guyon, I. and V. Vapnik. 1992. A training algorithm for optimal margin classifiers. In Proceedings of the Fifth Annual Workshop on Computational Learning Theory, pp. 144–152. ACM Press.

[Burges, 98] Burges, C. J. C. 1998. *A Tutorial on Support Vector Machines for Pattern Recognition*. Data Mining and Knowledge Discovery, 2(2), pp. 955-974.

[Cortes, 95] Cortes, C. and V. Vapnik. 1995. Support-vector network. Machine Learning 20, pp. 273–297.

[Dong, 01] Dong, X. and W. Zhaohui. 2001. *Speaker recognition using continuous density support vector machines*. Electronics Letters. 37(17), pp. 1099-1001.

[Jang, 07] Jang, R. 2007. Audio signal processing and recognition. http://140.114.76.148/jang/books/audioSignalProcessing/index.asp. Last verified: September 27, 2007.

[Lalonde, 07] Lalonde, J.F. and N. Vandapel. 2007. *Data Structures for Efficient Dynamic Processing in 3-D*. International Journal of Robotics Research, 26(8), pp. 777—796.

[Noll, 06b] J. Noll, F. Kileng, R. Hinz, D. Roman, M. Pilarski, E. Lillevold. 2006b. Semantic Service Delivery for Mobile Users. Proceedings of WWRF #17 meeting, WG2, Heidelberg, 15.-17.11.2006.

(Please check if this is the correct reference – it was not given in the text – J Noll references are available from the link below)

http://wiki.unik.no/index.php/Unik/JnollReferences

[Shannon, 05] Shannon, B.J. and K. K. Paliwal. 2005. Influence of autocorrelation lag ranges on robust speech recognition. ICASSP 2005, pp. 545 – 548.