A COMPETENT POST-AUTHENTICATION AND NON-REPUDIATION BIOMETRIC-BASED SCHEME FOR M-LEARNING

Georgios Kambourakis and Dimitrios Damopoulos
Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean
Karlovassi, GR-83200 Samos, Greece
{gkamb, ddamop}@aegean.gr

ABSTRACT
As mobile learning (mLearning) gains momentum, so does the worry of the parties involved to mLearning activities regarding the security and privacy level of the underlying systems and practices. Indeed, the basically spontaneous nature of mLearning and the variety of out-of-control devices that are used for supporting its activities, makes it prone to a plethora of attacks such as masquerading and man-in-the-middle. Thus, the provision of some sort of post-authentication and non-repudiation service in an effort to deter and repel ill-motivated activities may be of particular value in such realms. Compelled by this fact, in this paper, we introduce a dynamic signature-based biometric scheme to enable the offering of both of the aforementioned services in mLearning domains. We argue that our solution is both practical and lightweight. Its feasibility is also demonstrated through the use of machine learning techniques.

KEY WORDS
mLearning; Authentication; Non-repudiation; Security; Biometrics.

1 Introduction

With the proliferation of mobile devices and the increasing capabilities of modern smartphones, mobile learning (mLearning) is getting a lot of attention. So far, most mLearning advances have concentrated on course development, deployment and delivery, paying little attention to security and privacy. However, these issues are important to any educational context given that mLearning gains in popularity and more and more individuals are using its services on everyday basis. Specifically, mLearning systems allow multiple users to upload, download, and exchange information anytime, anywhere. So, there are many important security and privacy parameters that must be taken into careful consideration; authentication, access control, data integrity, non-repudiation, content protection, to name just a few. For instance, an evident challenge is to constantly track the persons accessing the mLearning content and to monitor their true identity (authentication). This is also known as post-authentication and refers to the situation where authentication is performed repeatedly after a successful login. Post-authentication is of particular importance for mLearning because it allows for constant tracking and identification of the initially authorized user and thus enable educators and course administrators to detect misuses.

A closely related issue to authentication in general is that of non-repudiation. This refers to an authentication that with high certainty can be claimed to be original. In the context of this paper this means that the person making a transaction, say, submits a test answering sheet, is not in position to deny this act at a later time. Also, from the evaluator's point of view, it means that they can rest assure that the transaction has been performed by the original submitter, that is, the person who was initially authenticated and authorized to do so. Thus, non-repudiation is about obtaining a proof that the announced participant really performed a given transaction and that this proof can be verified even without the consent of the said submitter. In this respect, non-repudiation cannot be imposed by means of symmetric cryptography since verification can be done without the submitter's consent and thus it cannot use whatever credentials (e.g., secret keys, passwords etc) the submitter may own. Therefore, non-repudiation usually mandates the use of some sort of Public Key Infrastructure (PKI). After that, non-repudiation can be realized by the use of digital signatures that act much like a written signature. This situation also requires that all participants own a digital certificate which bounds their public key with their true identity. It is also to be noted here that non-repudiation is also a legal concept, meaning that what technically is claimed to offer true non-repudiation may not stand strong in a court of law.

In any case, although the provision of non-repudiation may be of prime importance to eLearning - and imperative for other e-services such as m-Commerce - usually it can be more loosely defined for mLearning settings. This is because mLearning is more about learning, reference and exploration of information in a spontaneous (and often self-directed and self-starting) manner. For example, while in the airport lobby, one decides to take a short test in order to assess their level of comprehension over a given subject. In this respect, mLearning is more about interacting with information at the moment they are needed and/or in a specific use context. This means that non-repudiation is desir-

able but usually not of top priority and the focus should be on deterring rather than catching the perpetrator. Putting it another way, it is commendable to have some sort of proof that for example the learner who uploaded the answers to an mLearning test is the person to which the test is delivered in the first place, but we can do so with a certain amount of confidence, say, above 90%. Of course, the more rigorous the context is (e.g., participation to a formal examination) the greater the amount of confidence needed to verify the act. So, for mLearning realms, non-repudiation should be simple for the end-user and practical to implement. In this respect, the use of PKI may be not the proper solution as it is certain to impose high deployment and administration costs [1]. Also, it requires substantial processing resources from the end-user device which at least for the time being may be not the case for several smartphone models, especially the cheap ones.

Motivated by this fact, in this paper we propose a fair post-authentication and non-repudiation scheme for mLearning. Our scheme can be straightforwardly applied to devices equipped with a touchscreen and is based on dynamic signature. This is a biometric modality that exploits the anatomic and behavioral characteristics that a person exhibits when writing on a touchscreen - using their finger or a pen - a given phrase or signing their signature. The proposed scheme requires minimal effort form the end-user as they only need to submit: (a) upon registration (enrolment) to the mLearning portal, a dynamic signature sample of a random string presented to them by the server, and (b) after every sensitive mLearning transaction (one that requires non-repudiation) reproduce a dynamic signature of the same string. It is also relevant to note that by offering non-repudiation we also enforce post-authentication per sensitive transaction on the service-side. Specifically, only the legitimate learner is able to produce the correct dynamic signature. So, it is highly probable that the transaction has been performed by the initially authenticated person (e.g., by means of username/password) and not from a non-authorized user or an impostor. We capitalize on machine learning and though experimentation we demonstrate that our scheme is able to correctly classify a dynamic signature in an amount that exceeds 95%.

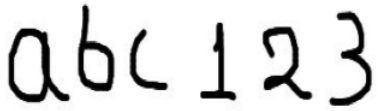
The rest of the paper is organized as follows. The next section addresses related work on the topic. Section 3 provides a high-level description of the proposed dynamic signature scheme. Section 4 details on the feasibility of the proposed solution. The last section concludes and outlines future work.

2 Related work

It is true that until now several works in the literature address the issues of security and/or privacy in the context of eLearning. For the interested reader, an overview of this topic can be obtained from [2, 3, 4, 5, 6, 7, 8, 9, 10, 11]. The same issues are also identified by some researches but specifically for the mLearning realm [12, 13, 14, 15]. In the following we briefly survey closely related work with particular emphasis on biometric-based schemes proposed to cope with the issues of authentication and non-repudiation in e/mLearning settings. First we address non-biometric-based solutions and then those that exploit some sort of biometric technology.

The authors in [16] try to tackle the issue of arbitration in eLearning contestation processes and propose a non-repudiation system for student evaluation based on web services. They capitalize on Asynchronous JavaScript (AJAX) frameworks and PEAR packages aiming to implement Extensible Markup Language (XML) security standards to provide improved user experience, asynchronous data exchange and message authentication for on-line test papers. The work in [17] also utilizes XML security standards such as XML Encryption and Signature in an effort to provide secure mobile Wiki services. By capitalizing on Web services technology the authors in [18] introduce a security service, namely INCA, to support security requirements of different eLearning systems. The proposed security service makes use of asymmetric cryptography and digital signature to support integrity, non-repudiation, confidentiality and authenticity in collaborative education environments, regardless the architecture in which they were developed.

The use of biometrics in eLearning settings is an aspect that has not been completely ignored by researchers [19]. Specifically, the works by [20, 21] describe some possibilities of using biometric features and solutions in the field of eLearning and propose to combine several different biometric methods toward this goal. The authors in [22] propose the use of random fingerprint biometrics user authentication during e-examination procedures. The work in [23] argues that multi-biometrics can be proved very handy for improving the reliability of biometrics authentication when a single biometrics authentication technology is not sufficient. Hence, the authors propose an authentication system that exploits multi-biometrics to support various services in eLearning where user authentication is required. The use of webcam face images to authenticate the presence of users during on-line courses is addressed by the work in [24]. Also, the authors in [25] introduce a biometric scheme for providing continuous user authentication in e-examination through keystroke dynamics. The work in [26] proposed a fingerprint-based method for conducting e-examination in a way that no unauthorized individuals are permitted to upload submissions or access information. The authors in [27] deal with the problem of tracking individuals accessing the learning materials and more specifically that of monitoring the true identity of the examination attendees and propose a multimedia-enriched interactive non-repudiation system involved in a mLearning environment. They developed an application layer non-repudiation system based on a person's single biometric information (e.g., iris, fingerprint, face, or voice), which resulted in the generation of a unique digital ID per user. After that, digital signatures were created based on the digital IDs to provide message integrity and non-repudiation.



B&167.0&164.0&1344239437.941613
M&164.0&160.0&1344239437.971502
M&161.5&157.0&1344239437.988079
M&158.5&155.5&1344239438.003825
M&155.0&154.0&1344239438.019078
M&151.5&153.0&1344239438.035658
M&147.5&153.0&1344239438.051984
.....
M&129.5&180.0&1344239438.212103
M&129.5&183.0&1344239438.227871
E&130.0&188.0&1344239438.243741

This subset of records corresponds to the touch gesture of a given user to form the letter 'c' in the dynamic signature above. The gesture started at point (167,164) on Aug 06, 2012 at time 07:50:37 GMT and finished at point (130, 188) on Aug 06, 2012 at time 07:50:38 GMT (B = Begin, M = Move, E = End. The character & is used as a separator between the fields).

Figure 1. A set of records created by the application for a given user when entering (signing) the letter 'c'

From the above analysis we can conclude that the non-biometric solutions proposed so far to cope with the issues of post-authentication and/or non-repudiation are either PKI-based [18] or concentrate on some kind of high layer custom-tailored solution like XML security [16]. However, as already pointed out, PKI is not a straightforward solution especially for mLearning domains as it imposes high deployment and administration costs and directly affects interoperability. Application layer solutions, while highly customizable, are usually platform-dependent. So, they require special effort to become cross-operable and interoperable. On the other hand, most of the biometric solutions proposed so far either require special equipment to be deployed in certain places [24], or impose the use of expensive equipment [22], [26], [27]. A major problem of biometrics authentication (like Keystroke [25] and mouse clicking) is that it is not free from errors and false recognition rate can be very high. Multi-biometrics as proposed in [23] is a solution to this problem but adds significant costs to the system in terms of complexity and (un)manageability. Also, it augments the acquisition cost of the mobile equipment if for example a high resolution camera or fingerprint sensor is needed.

So, under the assumption that in most cases mLearning does not impose absolute ceilings on post-authentication and non-repudiation we can argue that the ideal system to provide such services should be practical for the end-user, easy-deployable, cost-effective, scalable, and platform-independent. As discussed in the following sections, the proposed scheme fulfills the aforementioned requirements, while being highly accurate in identifying correctly the legitimate user, and thus generating the required proof to support non-repudiation. Also, to the best of our knowledge, this is the first study to explore the potentiality of dynamic signature in ultramodern smartphones equipped with a touchscreen.

3 System Description

Our proposal follows a simple and lightweight client-server architecture, where the latter entity is considered to be trusted. The communication link between these entities is also reckoned to be secure, e.g., by means of the *https* protocol. The client is assumed to carry a smartphone or tablet equipped with a touchscreen. Normally, the client has some kind of trust relationship with the server. This relationship is usually materialized in the form of some login credentials, say, username/password. The exact (out of band or online) way these credentials are acquired are out of the scope of this paper. After the very first login, the client is prompted with a random string (e.g., *abc123*) which the m-learner must 'sign' 3 successive times using their finger or stylus pen on its device. Upon completion, the answer containing all three dynamic signatures of the same string is sent back to the server which univocally registers these samples of dynamic signature with the corresponding user. This step is mandatory to be executed only once upon registration to the service.

A prototype of the proposed system has been implemented in iOS (formerly known as iPhone Operating System). Figure 1 depicts how such a dynamic signature is recorded by our application in the device. Each character of the dynamic signature is formed by one or more touch gestures. So, in essence, each gesture can be represented by a series of quadruplets in the form $\{Type, X, Y, Time\}$, where Type corresponds to the type of the movement, X, Y hold the Cartesian coordinates where the touch event took place, and Time carries the date and time (based on seconds since the standard epoch of 1/1/1970) the touch event occurred. Taking Fig. 1 as an example, the letter 'c' for this user is recorded as a series of finger or stylus pen movements in the context of a single gesture that began (B) at point (167,164) and ended (E) at point (130,188).

The letter M is used for records that represent inter-

Figure 2. A screenshot of the graphical user interface displayed to the instructor when reviewing a test

mediate points of the same (still) on-going gesture. So, overall, a complete signature is not stored as an image but it is actually comprised of several tens of quadruplets.

As already pointed out, once the initial registration phase has been carried out, the client is ready to participate in any sensitive transaction with the server. Some examples of such situation are: download learning material that requires proof of acquisition, download copyrighted material, post their contribution to a restricted forum, upload an essay, carry out e-examination tasks, etc. Let us assume a situation where the user has received a test containing different types of test questions. As soon as it is received, the test must be completed and sent back, say, within 20 minutes. At the end of the test there exists a verification string (the same with that the user submitted to the server upon registration) which the user must also 'sign' on the device's touchscreen before submitting the test back to the server. Upon reception, the server automatically compares the signature received with that contained in its database and makes an assessment, in terms of a percentage value, on whether the signature is authentic. It also automatically attaches this value to the test for informing the instructor about the result. The instructor (evaluator) is able to login to the server and download the completed tests to their mobile device or desktop computer for reviewing and evaluation. The system displays on the upper right corner the result of the verification process regarding the signature. This result (degree of confidence) is calculated as the quotient of how many points of the submitted signature have been found to match with the existing profile of the same user divided by the total number of points contained in that dynamic signature. In our proof-of-concept implementation we display this result in green if the calculated confidence percent is is slightly above 98,3%, in red if the result is marginally below 97%, and yellow otherwise. The way these percentages are derived is explained further down in section 4.2. In the latter case (yellow), the decision whether the instructor will accept the test as genuine or not is entirely up to her. To exemplify these, in Fig. 2 we present a screenshot of a completed test as displayed in the iPad device of the examiner.

It is also to be noted here that the proposed scheme may be useful not only for mLearners but for other contributors to the system as the case may be. For example, the instructors may be also bound to submit their personal dynamic signature string when making sensitive transactions such as uploading test results or downloading copyrighted content. This way, masquerading or man-in-the-middle attacks can be effectively deterred and repelled.

4 Evaluation

In this section we capitalize on machine learning techniques to assess the effectiveness of our scheme in correctly classifying a signature. This process provides evidences of the potentiality of the proposed solution to correctly identify a user. First, we detail on the methodology followed and next concentrate on the evaluation results obtained.

Table 1. Dynamic Signature-based classification results

	% FAR	% FRR	% EER
Bayesian Networks	1.6	6.6	4.1
RBF	2.9	16.2	9.5
KNN	0.5	3.7	2.1
Random Forest	**0.2**	**3.2**	**1.7**

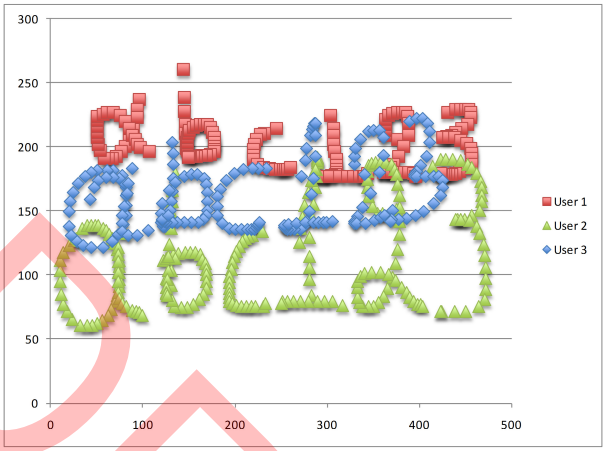


Figure 3. Cross-projection of the dynamic signature of the same string as entered by three different users

4.1 Methodology

As mentioned in the previous section we have implemented a prototype of our dynamic signature scheme in iOS. The application has been installed on the iPhone device of 20 participants (iPhone owners).

Each person used its device for registering with the server, that is, by entering 3 successive times the same text namely 'abc123' with the help of the client application. Although in a real deployment each user will have a unique string to be used as their dynamic signature, here we employ the same string for all users aiming to assess the effectiveness of the system to cope with forgery. After the completion of the data collection process, the files containing the dynamic signature data were used to assess the effectiveness of the proposed scheme. Recall that each signature file contains an arbitrary number of records where each of them corresponds to a vector of related features per signature.

For the needs of the classification process, 20 data files – one per user – have been created. Each of these files contains the signature data of the corresponding legitimate user and the data of the rest 19 users that represent potential intruders. Specifically, for each user in the dataset, the corresponding data file contains: a) the user's data, referred to as normal behavior data, and b) all other users' data that represent potential intrusive behaviors. Each record of the signature data file is composed of collected features represented by the following quintuplet: {*Type, X, Y, Timestamp, Legit /Intruder*} where the last field is the binary representation of the two nominal classes, i.e., if this piece of data belongs to the legitimate user (yes) or the intruder (no). An example of such a record is given by the following quintuplet {*B, 167.0, 164.0, 1344239437.941613, yes*}.

During the experiments we cross-evaluated four supervised machine learning algorithms, namely, Bayesian Networks, Radial Basis Function (RBF), K-Nearest Neighbor (KNN) and Random Forest. Moreover, the k-fold cross-validation method, and more specifically a 10-fold one (this option provides us with more chunks of data to work with), has been employed to divide the dataset into different subsamples. This means that the original sample is randomly divided into k (nearly) equally sized sub-samples, and the cross-validation process is repeated k times (the folds). Every time, one of the k sub-samples is used as the test set and the other k-1 are put together to form the training set. Finally, as discussed in the next section, the average value of all metrics across all k trials has been calculated. The experiments have been carried out using the well known machine learning software package, namely RapidMiner [28].

4.2 Results

Legacy biometric systems effectiveness analysis makes use of two error rates, namely False Acceptance Rate (FAR) in which an intruder is accepted by the system, and False Rejection Rate (FRR) in which the authorized user is rejected

by the system [29]. In addition, a third metric known as Equal Error Rate (EER) is generally employed to examine the performance of similar to ours biometric systems (e.g., keystroke systems) [30]. Specifically, EER is a kind of percentage rate which both accepts and rejects errors as equals (*EER=(FAR+FRR)/2*). This metric is employed to quantify the detection accuracy by a single number. The lower the error rate value, the higher the accuracy of the system. In our analysis we consider all the three aforementioned metrics to estimate the effectiveness of our dynamic signature-based scheme in correctly classifying a signature.

Table 1 summarizes the results obtained from the experiments. Random Forest seems to be the most promising classifier showing optimal results and having the lower EER among all the algorithms tested. More precisely, its average FAR, FRR percentage values remain near 0.2% and 3.2% respectively while the average EER for all cases is 1.7%. Bayesian Networks and KNN also show very promising results reporting an average EER of 4.1% and 2.1% respectively. On the contrary, RBF scores the highest errors rejecting the authorized user with a statistical average FRR of 9.5%. Overall, the results suggest that Random Forest is the best choice for implementing the proposed dynamic signature scheme. In practice, and in addition to what is described in section 3, these results mean that in a real implementation of the system the optimal value for accepting/rejecting a signature is that of 98.3% (*100 - EER%*) and 96.8% (*100 - FRR%*) correspondingly. For example, in the latter case (rejection), a signature is discarded if four of its points are found to be inconsistent with that contained in the profile of the corresponding legitimate user.

As a general remark, dynamic signature-based classification presents significantly better results compared to those reported in the literature so far. It is also to be noted that while these results provide strong evidences that dynamic signature-based classification may be a very accurate means of authenticating the user, more research is needed to better assess its potential. To further exemplify the above findings, in Fig. 3 we cross-projected the dynamic signatures of the sample string as entered by three different users. Bear in mind that each signature is actually a series of Cartesian coordinates as recorded in the corresponding signature file for that user. From the figure, it is obvious that each signature is to far from being characterized as similar to the others.

5 Conclusions and future work

This paper addressed the issues of post-authentication and non-repudiation in the mLearning realm. We proposed a biometric scheme based on dynamic signature to support the provision of both of these services in a practical and efficient manner. The only actual requirement for our solution to work is the end-users to afford a mobile device equipped with a touchscreen. By using a prototype implementation we showed that the proposed solution can be very accurate in correctly classifying a signature and thus providing strong evidences that a given transaction has been performed by the legitimate user. The lightweight nature of our proposal is also self-evident as requires no additional computational resources on the client-side (recall that the dynamic signature data is recorded and transferred as text).

Nevertheless, some aspects of the solution need further research. For instance, the physical characteristics of a device and in particular those of the touchscreen (especially its size) may affect efficiency. So, more research effort is needed to examine how the scheme will behave if a user employs different devices in its mLearning activities (or decides to replace her device with a new one). The use of different means (e.g., finger, stylus pen) to produce the dynamic signature is also an issue worthy of investigation.

References

[1] K. Park, H. Seok & K. Park, pKASSO: Towards Seamless Authentication providing Non-Repudiation on Resource-Constrained Devices. *Proc. 21st IEEE Symposium on Pervasive Computing and Ad Hoc Communications*, 105-116, 2007.

[2] S. Furnell, U. Bleimann, J. Girsang, H. Rder, P. Sanders & I. Stengel. Security considerations in online distance learning. *In Proc. of Euromedia 99*, Germany, 31135, 1999.

[3] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, Privacy and security in e-learning, *International Journal of Distance Education, 1*(4), 2003.

[4] E. Weippl, Security in ELearning, *Volume 6 of Advances in Information Security*, Springer Science + Business Media, Inc., 2005.

[5] J. Castella-Roca, J. Herrera-Joancomarti & A. Dorca-Josa. A Secure E-Exam Management System. *In Proc. of the First International Conference on Availability, Reliability and Security (ARES '06)*, IEEE Computer Society, USA, 864-871, 2006.

[6] G. Kambourakis, D. P. Kontoni, A. Rouskas & S. Gritzalis, A PKI Approach for Deploying Modern Secure Distributed e-learning and m-learning Environments, *Computers and Education, 48*(1), 1-16, 2007.

[7] J. Yong, Security modelling for e-Learning. *First IEEE International Symposium on Information Technologies and Applications in Education (ISITAE '07)*, 2007.

[8] J. Mwakalinga, L. Yngstrm & S. Kowalski, Securing e-learning system using a holistic and immune security framework. *The 4th International Conference for Internet Technology and Secured Transaction (ICITST '09)*, London, UK, 2009.

[9] P. R. L. Eswari, A process framework for securing an e-Learning ecosystem. *International Conference for Internet Technology and Secured Transactions (ICITST '11)*, 403- 407, 2011.

[10] J. C. Granda, P. Nuno, D. F. Garcia & F. J. Suarez, Security Issues in a Synchronous e-Training Platform. *Sixth International Conference on Availability, Reliability and Security*, 485- 492, 2011.

[11] D. Costinela Luminita, Information security in E-learning Platforms, *Social and Behavioral Sciences, 15*, 2689-2693, 2011.

[12] E. R. Weippl, Security considerations in m-learning: threats and countermeasures, *Advanced Technology for Learning, 4*(2), 99-105, 2007.

[13] Zsolt Ugray, Security and privacy issues in mobile learning, *International Journal of Mobile Learning and Organisation, 3*(2), 202-218, 2009.

[14] M. K. Titi & O. A. Marie. 2009. Protecting E-courses Copyright in M-learning Process. *Proc. of the 2009 International Conference on Future Computer and Communication (ICFCC '09)*, USA, 636-640, 2009.

[15] J. Yong, Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes, *Journal of Universal Computer Science, 17*(2), 296-310, 2011.

[16] R. A. Buchmann & S. Jecan, An arbitration web service for e-learning based on xml security standards, *WSEAS TRANSACTIONS on COMPUTERS, 10*(7), 1742-1751, 2008.

[17] C. Kolias, S. Demertzis, G. Kambourakis, Design and implementation of a secure mobile wiki system, *Proc of the Seventh IASTED International Conference on Web-based Education (WBE '08)*, 212-217, 2008.

[18] T. de Medeiros Gualberto, Service for secure and protected applications in Collaborative Learning Environments, *IEEE International Conference on Systems Man and Cybernetics (SMC '10)*, 2419- 2426, 2010.

[19] Q. Gao, Online teaching: Do you know who is taking the final exam?, http://www.asee.org. Accessed 16 August 2012.

[20] K. Rabuzin, M. Baca & M. Sajko(2006). E-learning: Biometrics as a Security Factor. *International Multi-Conference on Computing in the Global Information Technology (ICCGI '06)*, 64-64, 2006.

[21] S. Asha and C. Chellappan, Authentication of e-learners using multimodal biometric technology. *International Symposium on Biometrics and Security Technologies*, 1-6, 2008.

[22] Y. Levy & M. M. Ramin, A Theoretical Approach for Biometrics Authentication of e-Exams, http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

[23] S. Asha, Authentication of e-learners using multimodal biometric technology, *International Symposium on Biometrics and Security Technologie (ISBAST '08)*, 1- 6, 2008.

[24] B. E. Penteado & M. N. Aparecido, A Video-Based Biometric Authentication for e-Learning Web Applications, *Enterprise Information Systems. Lecture Notes in Business Information Processing, 24*(4), 770-779, 2009.

[25] E. Flior & K. Kowalski. Continuous Biometric User Authentication in Online Examinations. *Seventh International Conference on Information Technology*, 488-492, 2010.

[26] S. Alotaibi, Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. *The 4th Saudi International Conference*, UK, 2010.

[27] S. Adibi, A remote interactive non-repudiation multimedia-based m-learning system, *Telematics and Informatics, 27*(4), 377-393, 2010.

[28] Rapid-I, RapidMiner, http://rapid-i.com/

[29] F. Bergadano, D. Gunetti & C. Picardi, User authentication through keystroke dynamics. *ACM Transactions on Information and System Security, 5*(4), 367-397, 2002.

[30] R. Giot, M. El-Abed & C. Rosenberger, Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis, *The Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '12)*, 2012.