# RESUMEN DE TESIS DOCTORAL

# Design and Implementation of an Advanced Security Remote Assessment System for Universities Using Data Mining

## *Diseño e Implementación de un Sistema de Evaluación Remota con Seguridad Avanzada para Universidades Utilizando Minería de Datos*

**Graduated: José Alberto Hernández Aguilar**
Centro de Investigacion en Ingeniería y Ciencias Aplicadas (CIICAp)
Universidad Autónoma del Estado de Morelos (UAEM)
jose_hernandez@uaem.mx
*Graduated on November 28, 2008*

**Advisor: Gennadiy Burlak**
Centro de Investigacion en Ingeniería y Ciencias Aplicadas (CIICAp)
Universidad Autónoma del Estado de Morelos (UAEM)
gburlak@uaem.mx

**Advisor: Bruno Lara**
Facultad de Ciencias
Universidad Autónoma del Estado de Morelos (UAEM)
bruno.lara@uaem.mx

**Abstract**
We develop the detailed application of the computer technology on testing the student's level of knowledge. We implemented a Java original code, client-server technology based on the natural process of evaluation where the college students (clients) are tested for an examiner (server). Later, we discuss the security measures implemented by leading suppliers of e-learning tools, and we distinguish an important opportunity area on the use of advanced security measures that we used to differentiate our tool. Then, we present a data mining methodology to analyze activities of students in online assessments to detect any suspicious behavior (cheating), and show the results of applying it on a real class. Finally, we propose an affordable biometric technology to recognize remote students in online assessments to solve the well-known problem of: "who's there".
**Keywords:** Online Aassessment System, Data Mining, Advanced Security, Biometry.

**Resumen**
Desarrollamos una aplicación de la tecnología computacional en la evaluación del conocimiento de los estudiantes. Implementamos una tecnología cliente-servidor, de código original en Java, basada en el proceso natural de evaluación donde los estudiantes (clientes) universitarios son evaluados por un examinador (servidor). Mas adelante, discutimos las medidas de seguridad implementadas por los proveedores líderes en herramientas de e-aprendizaje, y distinguimos una importante área de oportunidad en el uso de medidas de seguridad avanzada que usamos para diferenciar a nuestra herramienta. Entonces, presentamos una metodología de minería de datos para analizar las actividades de los estudiantes en evaluaciones en línea para detectar cualquier comportamiento sospechoso (trampas), y mostramos los resultados obtenidos de aplicarla en una clase real. Finalmente, proponemos una tecnología biométrica asequible para identificar a los estudiantes remotos en evaluaciones en línea para solucionar el bien conocido problema de: "¿quién está ahí?".
**Palabras clave:** Sistema de Evaluación en Línea, Minería de Datos, Seguridad Avanzada, Biometría.

## 1 Introduction

The psychologists distinguish two basic kinds of activity for the person involved on this process: the teaching and learning. The teaching is the activity objectively directed to independent development of the knowledge system and skills of the person. Learning is an activity of one person (the teacher) directed to management the activity of other person (the student). Nowadays, teaching techniques must be based on modern achievement of a science, as well as

the technologies. Therefore, modern training should do widely use of technology based on the application of computers [Bugai, et al., 1997]. The test as a tool for measurement of results of pedagogical work gets special importance, because without it the individual work with every person cannot be organized. On the other hand, the test serves the major tool of measurement of a level of knowledge and difficulty of the tasks. It is impossible to operate educational process especially in technological variant, without such tool [Carnegie, 2005; Hunt, et al., 2002; Varughese, 2005].

A basic question arise: Why to use online assessment? We can answer the following. Online assessment is a common practice around the world; more than 271,000,000 links at Internet search engine (similar Google.com) support this statement. However, is it really a good tool to assess persons? Can we trust on results? Can we trust on students? We can say online assessments are useful to evaluate the students' knowledge; they are used around the world for schools -since elementary to higher education institutions- and recognized training centers of very important companies like the Cisco Academy. Solving second and third question is not easy, in traditional tests "copying from another student during a test" and "using banned crib notes or cheat sheets during a test" is categorized by the students as cheating [Cavalli, et al., 2005] and several research [McCabe, et al., 1996] have shown is a common practice. Scenario changes drastically when exams can be done remotely through the Internet [Morris, 2005; Rove, 2004]. One of the basic problems to solve is to know: who is there?

### Problem at hands

The main purpose of this paper is to implement an Online Testing System (from now indistinctively OTS) to assess the students' basic knowledge through on-line assessments over client-server technology. The original character of this project is focused on the proposal to substantially improve security mechanisms implemented in on-line assessment systems by means of artificial intelligence techniques, specifically the use of data mining to detect student cheating, and the use of biometric recognition to identify remote students; elements that already have not been implemented on current leading assessment tools.

### Structure of the document

First, we present a mathematical model that supports the validity of the on-line assessment by means of a computerized tool, then we described the performance of our proprietary Online Testing System. Later, we analyze the leading assessment tools on the market and identify a niche for the advanced security mechanisms, based on this analysis we present our two innovative approaches to deal with advanced security in online assessments: 1) data mining to detect on-line student cheats and suspicious behavior, and 2) identifying remote students by means of biometry to solve the well-known question of who is there?; we discuss our results, and finally we present our conclusions and future work.

## 2 Grade as the evaluation of the Student's basic knowledge level

In our analysis, we pay main attention to the closed-ended form or the tests. We assume that the levels of the knowledge are ordered as follows: the quantity $F_i$ is greater or equal with respect to other answers $F_i >= \overline{f}_{ij}$ . We suppose that it is only the unique right answer to every question in the etalon collection. Further we renormalize $\overline{f}_i$ and $F_i$ with some coefficients $w_i$. With the use $w_i=1/F_i$ the etalon knowledge is represented by a straight line $F_i=1$, while the student knowledge is rewritten as $\overline{f}_{ij}/F_i = f_{ij}$, where $0<= f_{ij} <=1$.

In Fig.1 are shown schematically two distributions: the etalon knowledge and the student knowledge. The line at the top represents the level of correct (etalon) knowledge (The teacher's knowledge), and the variant line the student's knowledge. $X$-axis corresponds to the number of asked question, while in the $Y$-axis the level of student's answer is postponed.

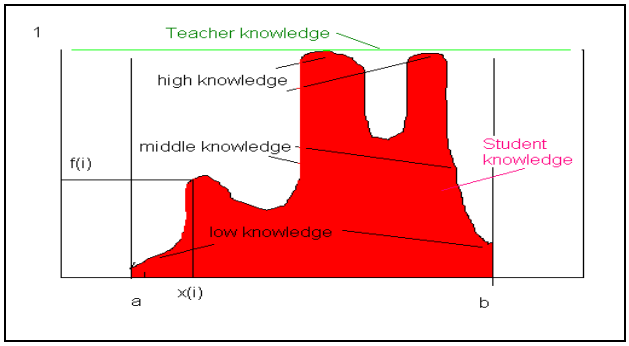


**Fig. 1.** Distribution of normalized etalon KB (Teacher knowledge) and distribution of student's KB (correct, wrong) in general (variant line)

By considering above described, according [Burlak, et al., 2006] the normalized knowledge of student is

$$Z_s = \frac{1}{N}\sum_{i=1}^{N} f_i \tag{1}$$

In the framework of the knowledge measurement, the following factors are important: (i) For the objectivity of the estimation the student should not be foreknown on the sequence of the asked questions. This means that the order of the records in the task (both questions and predefined answers) should be randomized. (ii) The number of questions should be large enough to achieve of the desired accuracy of evaluation.

In result the student's knowledge after the test may be represented as

$$Z_s = \frac{1}{n}\sum_{i=1}^{n} f(\xi_i) \tag{2}$$

where the integer numbers $\xi_j$ already are not the successive integer numbers of the questions in the initial collection, but the random integers distributed in $[1, N]$. With Eq.(2) the problem of the knowledge measurement may be redefined as the problem of numerical evaluation of the sum $Z_s$.

## 3 Proprietary Online Testing System

We present the dynamic interaction of the OTS (see Fig. 2). At left side is the Server, at right side the Client -or Clients-. Before any Client can be connected, the Server must be at listening mode. To start the evaluation process, the Client needs being validated into the Server, if this is a valid one, then receives a collection of assessment items (tasks) from the Server containing the questions in the test. These assessment items are displayed in the Question and Test (Q&T) interface, and the client starts the assessment, each assessment item is shown and the Client must select an answer, when the test is finished, it is processed at the Server side, and then the results are sent to the Client side to be displayed. The process of evaluation can be repeated several times in training mode and just one time in control mode.

Server side and client side are multi platform (were developed on Java), Server allows students to be tested from remote places or in local area network [Burlak, et al., 2005a]. Our OTS shows the test's questions and the answers in a random way. Each question has assigned a time to be answered (depending on the difficulty level), and do not permit to go back to the previous questions.

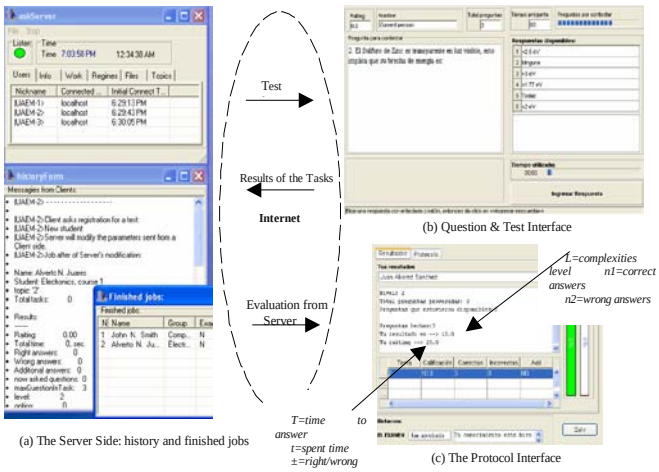


**Fig. 2.** Dynamic Schema, The Server side is attending Clients [Burlak, et al., 2005]

## 4 Educational Security

Since problems of information security are so common today, it is not surprising that problems of "educational security" could be common too. Regarding this issue, in [Hernandez, et al., 2006] is documented a wide spectrum of techniques to commit cheat in online assessments. However the main problem in online assessments is to know who's there [Wisher, et al., 2005].

**Table 1.** Classification of security measures in common e-learning tools. - = Not specified

| Software tool | Black board | Question Mark | Perception |
|---|---|---|---|
| **BASIC SECURITY** | | | |
| Login names and passwords | Yes | Yes | Yes |
| Control time in assessment process | Yes | - | - |
| Restrictions on the number of times a learner can take a test | Yes | - | - |
| Randomly selection of assessment items from a database pool/Randomly order of answers | Yes | Yes | Yes |
| Tests at a specified time and date | Yes | - | - |
| **ENHANCED SECURITY** | | | |
| Avoid Windows Hot keys | No | Yes | Yes |
| Function that prevents learners from closing the test when using other computer applications or surfing the Web while the assessment is in progress | No | Yes | Yes |
| Disabled print buttons/Test unprintable | No | Yes | Yes |
| Removes standard browser toolbars | Yes | - | Yes |
| Use of PhotoID for live proctoring | Yes | - | - |
| Limit save-to-disk functions | No | Yes | - |
| Role based security | Yes | Yes | - |
| Encryption of information or encapsulation of data on web form | Yes | - | - |
| During an assessment answers can be "auto-saved" | No | Yes | - |
| **ADVANCED SECURITY** | | | |
| Use Biometry to identify remote students. | No | No | No |
| Use of Data mining to detect students cheating. | No | No | No |

### 4.1 Classification of security measures

Fortunately, online assessment providers [Blackboard, 2006; QuestionMark, 2009; Pearson, 2006] among others have implemented several mechanisms to deal with educational security. We have classified these mechanisms into three security levels: basic, enhanced and advanced (see Table 1).

The above described software tools provide some basic and enhanced security measures to ensure security in on-line assessments; however none provides any advanced security feature to support virtual proctoring.

## 5 Use of Data Mining to Detect Students Cheating and Suspicious Behavior

Have you ever commit cheat in an exam? an if so, why? In a sample of 1,800 students at nine state universities in United States of America, seventy percent of students admitted to cheating on exams [McCabe, et al, 1997]. According [Rove, 2004] in online assessments in which we are not sure who is taking the test; students will be under pressure, some students perform unfairly poorly under pressure and this is a good incentive to cheat.

### 5.1 Data Mining to Detect Cheats (DMDC) in online assessments

Data mining has been successfully used to analyze student behavior [Jing y Derrick, 2003; Van Horn, 1998]. We propose the use of Knowledge Discovery in Databases (KDD) a non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data for detecting student cheats in online exams. Ideally DME consists of a set of modules for tasks such as characterization, classification, cluster analysis, and evolution and deviation analysis. This process can be performed by means of Weka, and contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization [Ochoa, et al., 2006; Weka, 2005].

### 5.2 Methodology

We propose a five steps process to data mining databases containing responses of online assessments, surveys and historical information to detect cheats in on-line exams:

**1) Getting Data from students**. Information from students must be collected from the historical data and surveys.
**2) The evaluation process.** Carry out the student assessments using the OTS. To help reduce testing anxiety, you may consider offering practice quizzes with detailed feedback that do not count (or count very little) towards the students' grades. This provides a non-stressful way of practicing test-taking skills.
**3) Obtaining Feedback.** At the end of each exam the student will be is asked for feedback about exam, and also about the professor and examination conditions. Professor will fill respective on-line form. Data from student, professor and institutions will be is stored on the DB.
**4) Creation of the .arrf Data File.** Necessary data for Weka system will be obtained from DB, by using SQL statements and export facilities for further process.
**5) Data mining process.** This process includes: reading the .arrf file in the Weka Explorer system, proceeding to classify, visualize clusters and discover associations in the data [Ochoa, 2006]. Start the hidden patterns finding, remember to keep mind open (No prejudices).

### 5.3 Experiment

Second week of December 2005 we implemented the proposed methodology. We prepared the material for the final exam of Update on Information Systems subject, a 7$^{th}$ semester curricula (n=100) for the career of Computers and Managerial Systems. At the beginning of the semester, a student profile was prepared. On December 1$^{st}$ students were trained on the use of the OTS on class. On December 8$^{th}$ students were evaluated using the OTS with a fifteen, random, multiple choice test. Exam was automatically created from a sixty question database. The place for testing was the classroom and one of the computers was used as a Server. First attempt was on training mode, second attempt was done to assign a grade. In both cases students were supervised by their Professor. Students were asked about perceptions about exam and professor style. We used SQL statements and export facilities provided by MySQL to generate the .arrf data file, then we started data mining process with Weka.

### 5.4. Results

Data mining process revealed three clusters (see Figure 3): (a) the one of the advanced students 8.9% (who obtained good grades both on-line and in paper), (b) the average students 17.8% (who obtained better grades on the assessment in paper than in the on-line assessment), and (c) cheaters 73.3% (good or very good grades in the paper assessments and poor grades in the on-line assessment). When we analyzed the on-line grade versus rating (see Figure 4), we noticed that in the on-line assessment: the advanced students (a) responded well and in short time, the average students (b) responded in average times, but the students with low grades (c) responded in unacceptable times. Low GPA is associated to low ratting, then a contradiction appears, a student with low or poor knowledge is getting high off-line grades, this fact is really suspicious, the set of students fitting this cluster are cheating.

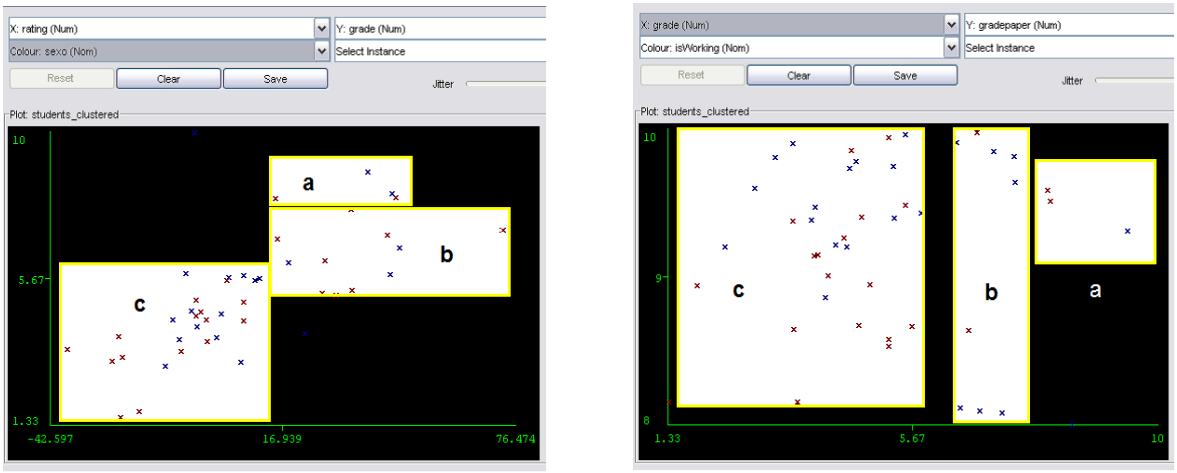


**Fig. 3 & 4**. On-line grade versus off-line grade, and student's rating versus on-line grade

### 5.5. Discussion

The environment of the evaluation was very controlled. Server and Clients were working on the same LAN, in addition the professor was always present during the examination doing almost impossible to commit trap. Nevertheless, when it is possible (case of the control examination), the students of low average (GPA), with weak knowledge, socially pressed to be successful committed trap. In this point a new question arises: What measures are due to take when we have detected students making trap? There are several actions that can be carried out, and may vary following the policies of each Institution, most important include: To expel the student and bulletin him/her through the Educative System; a warning and/or suspension of the student, if re-incidence then expel him/her; suspension of the student by a period of time (cases of impersonation) among others.

## 6 Use of fingerprint recognition to solve the question: Who is there?

We propose the use of biometrics, particularly the use of fingerprint recognition on real time to authenticate students into the assessment system, and web cam monitoring during online assessments to deal with the well-known problem of: who is taking the exam? We reviewed the literature on different related fields and we realized there exists several proposals to deal with this problem, however none documented implementations of such technologies has been tested with flesh and bone students.

### 6.1. The On-line Testing System with Biometric Recognition

Virtual proctoring involves using biometric technology to monitor students at remote locations. For virtual proctoring, is recommended using a layered approach depending on critical maturity of the test. With high stakes tests, video monitoring and a biometric measure such as iris scanning may be used. For medium stakes tests, a single biometrics measure may be acceptable [BSU, 2006]. Despite most of online assessments are located in the middle of both definitions, we consider the fact of high levels of cheating in remote assessments. In one hand, fingerprint recognition is a single biometric measure, the cheapest, fastest, most convenient and most reliable way to identify someone. And the tendency, due to scale, easiness and the existing foundation, is that the use of fingerprint will only increase [Tapiador y Singüenza, 2005]. Unfortunately, fingerprint recognition is used just to authenticate into systems, but then what? The student is free to use any media to commit cheat, to avoid that situation we considered the possibility to use web cams. Web cams are inexpensive and most of students are used to deal with them, they form part of their common tools to work and chat. Based on above exposed, we propose the mixed use of video monitoring, by means of web cams, and fingerprint recognition to provide a secure on-line assessment environment.

### Performance Schema (n-Tier C-S system)

In order to use fingerprint recognition, the first step is to enroll students –top, right side in Figure 5-, the students fingerprint is saved and indexed in the Features Database, In the features database is assigned the Student Personnel ID that is used to link the students' personnel information with the fingerprint image. The student enters to the on-line assessment application, and when system requires the user and password, his or her uses the Mouse Id –superior right side of Fig. 5- to scan his/her fingerprint.

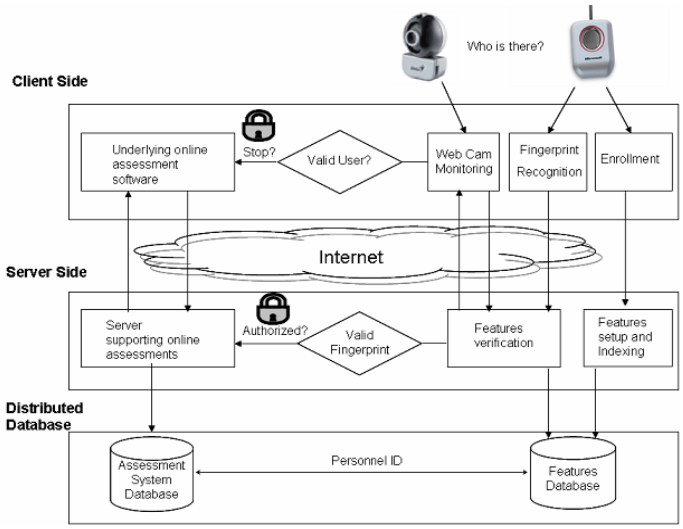


**Fig. 5.** Fingerprint recognition on real time in online assessments. Client (at top) and Server (at bottom)

The fingerprint is verified in the Features Database, and if it is recognized as a valid, then the Server authorizes access to the online assessment application, else an error message is sent to the Client to try again. In other hand, if the student's fingerprint is valid, the user is authenticated into system, the evaluation process starts and web cam transmission is initialized at Client Side to conduct real time monitoring by means of multitasking. If someone else tries to get the control of the computer during the online assessment, the evaluation process is finished prematurely, and the results are sent to server side to be processed as they are. To the contrary, the evaluation process is finished successfully, the assessment is processed at Server Side, and the final results of evaluation and security status are shown at Client Side. To implement this approach, we improved the OTS described in section 3 with multimedia management and fingerprint recognition features as described in [Hernandez, et al., 2008].

### 6.2. Methodology

For our experiment, we selected a random sample of students (n=102) from the José María Morelos y Pavón High School, located in Temixco, Morelos, México. We carried out two evaluations, a control evaluation (paper and pencil), and a second evaluation with our online assessment system with biometric recognition.

**- Tests design.** Tests were designed by professors on August 5th and 6th 2007, one of them was implemented for the online assessment using our authoring tool. The tests consisted of 30 questions with similar level of complexity, we evaluated arithmetic, algebra, geometrics, and trigonometric subjects.
**- Setting up.** Computers were prepared with our online assessment client software and biometric devices, network connectivity was tested.
**- The traditional test.** The paper and pencil test was conducted on August 14th 2007.
**- Enrollment.** Students were enrolled into the system by taking their left-hand index fingerprint on August 15th 2007. We took care of the students were identified by the system after their enrollment.
**- The online assessment with biometric recognition test.** Was conducted on the Computers Network Laboratory located at the High School facilities from August 16th to August 17th 2007, each computer used in the experiment had attached a Microsoft Fingerprint Reader, a web cam, a broad band connection to our server as well as our proprietary client system. First of all, Students were instructed in how to use the system, we explained them that a web cam was monitoring their activities, later students authenticate by means of their fingerprint into our Server System and the computerized assessment started. The use of calculator and cellular phones was avoided.
**- The Survey.** At the end of the exam we applied a survey to determine students' profile and perceptions about system's operation.
**- Statistical Analysis.** Data was processed using descriptive analysis, using relative numbers and percentages using Ccount gnu free software.

### 6.3. Preliminary Results and Discussion

On this test with obtain a FAR of 99.99% and a FRR of 97.09%, only one female student could not be recognized despite several trials. Her fingerprint template can not be understood by the system due her fingerprints seems like stains. Similar cases are registered in literature [Michigan Org, 2007]. We faced this problem by providing her an user and a strong password. The average grade in paper and pencil test was 3.8 meanwhile the online grade was 3.5, this difference is explained due an small percentage of students must improve their computer skills, we noticed that video games and chat could improve students' skills and performance in online assessments. In general, students perceived our system as faster, easy to use and secure, fingerprint recognition plays an important role in this last point. However, they dislike time limited answers, and 13% dislike web cam monitoring. They felt under pressure, get nervous and dislike being monitored or watched. A 20% noticed a way to commit cheat using a system like ours. We made in-depth analysis and discover that students with poor performance (low grades) are more willing to commit cheat.

## Future Work

This work is by no means complete, and could be benefited from a number of future research directions. First, Testing of the proposed technology in our research center and other institutions to measure the effectiveness of methodology and make required adjustments.

Second, we want compare the results obtained with Weka as DM engine with results obtained using other tools like Matlab and SPSS. Third, we want to improve human-computer interface and assessment methodology by analyzing students comments and users feedback as in [Ochoa, et al., 2008]. Four, Regarding biometric recognition, we want to improve facial recognition, due at this point of our research we can detect student's presence or absence only, and our intention is comparing face patterns automatically by means of photo Ids stored at our features databases. Finally, We want to test the newest fingerprint scanners included in mouses, keyboards and in some laptops and try to incorporate them to work within our system.

## 7 Conclusions

In this thesis we have studied the Data Mining (DM) as a tool to detect the student cheats in online assessments. Since the increasingly new technologies evolve, students are mastering cheating in online tests. We believe that DM can be used successfully to detect student cheats, and consequently to improve security in online assessments.

Biometric recognition is a promising technology to deal with the problem of who is there? in online assessments, this technology is very well accepted but must be improved to be perceived as unobtrusive. Online assessments are an useful tool in educational process, but students involved on it, besides being trained for a specific subject, require to develop computer skills to be really effective.

## References


1 **Blackboard (2006, agosto).** Security. Retrieved from http://www.blackboard.com/us/index.aspx

2 **BSU Ball State University (2006, agosto).** Technology assessment reports on The use of Biometrics in education. Retrieved from http://web.bsu.edu/dpmuller/biometrics/

3 **Bugai, Y., Burlak, G., Demchenko, A. & Kuz'menko, N. (1997).** On Application of Computer Technology Testing In Educational Process, *Conference Role of Universities in the Future Information Society RUFIS'97*, Prague, Czech Republic, 141-144.

4 **Burlak, G.N., Hernández, J.A. & Zamudio-Lara, A. (2005).** The Application Of Online Testing For Educational Process In Client-Server System. *CONGRESS: IADIS International Conference*, Lisbon, Portugal, vol. 2, 389-392.

5 **Burlak, G., Ochoa. A. & Hernández, J.A. (2005a).** The application of learning objects and Client-Server technology in online testing to measure basic knowledge level. In *CONGRESS: X. Simpósio de Informática, V Mostra de Software Academico da PUCRS*, Uruguaiana, RS Brasil, 51-58.

6 **Burlak, G., Hernández, J.A., Ochoa, A. & Muñoz, J. (2006).** The measurement of the Student's basic Knowledge obtained by means of computer assessments, *Special issue: Advances in Computer Science and Engineering*, *Research in Computing Science.* 23, 201-213.

7 **Cavalli, A., Magg, S., Papagiannaki, S. & Verigakis, G. (2005).** From UML models to automatic generated tests for the dotLRN e-learning platform, *Electronic Notes in Theoretical Computer Science* 116, 133-144. Retrieved form *http://www.elsevier.com/locate/entcs*

8 **Hernández, J.A., Ochoa, A., Muñoz, J. & Burlak, G. (2006).** Detecting cheats in online student assessments using Data Mining. *Dmin06*, Las Vegas Nevada, USA, 204-210.

9 **Hernández, J.A., Ochoa, A., Andaverde, A. & Burlak, G. (2008).** Biometrics in online assessments: A Study Case in High School Students. *18th International Conference on Electronics, Communications and Computers Conielecomp*, Puebla, Mexico, 111-116.

10 **Hunt, N., Hughes, J. & Rowe, G. (2002).** Formative Automated Computer Testing (FACT). *British Journal of Educational Technology*, 33(5), 525-535

11 **Jing, L. & Derrick, J. (2005, December).** Data Mining and Its applications in Higher Education. Retrieved from http://www.ebscohost.com/

12 **McCabe, D. L. & Trevino, L. K. (1996).** What we know about cheating in college: Longitudinal trends and recent developments. *Change*, 28(1), 28-33.

13 **McCabe, D. L. & Trevino, L. K. (1997).** Individual and contextual influences on academic dishonesty: A multi-campus investigation. *Research in Higher Education*, 38(3), 379-396.

14 **Michigan Org (2007, agosto).** Fingerprint Classification. Retrieved from http://www.reachoutmichigan.org/funexperiments/agesubject/lessons/prints_ext.html

15 **Morris, T. A. (2005, 30 de diciembre).** Cheating and plagiarism in the information age. Retrieved from http://terrymorris.net/tohe2004/CPIA_morris.pdf

16 **Ochoa, A. (2006).** *Más allá del Razonamiento Basado en Casos y una aproximación al Modelado de Sociedades Utilizando Minería de Datos.* Post Doctoral Thesis, State University of Campinas, Radamelli, SP Brazil.
17 **Ochoa, A., et al. (2006).** Italianitá: Discovering a Pygmalion Effect on Italian Communities. *Advances in Computer Science and Engineering*, 19, 57-67.
18 **Ochoa, A., Hernández, J.A., González, S., Castro, A. & Ponce, J.C. (2008).** Evaluating the Authority in a Weblog Community. *Computación y Sistemas,* 11(4), 370-380.
19 **Pearson (2006, agosto).** Pearson Online Assessment Software from Pearson Assessments. Retrieved from http://www.pearsonassessments.com
20 **QuestionMark (2006, agosto).** QuestionMark Perception Product Information. Retrieved from http://www.questionmark.com/us/perception/
21 **Rove, N. C. (2005, 30 de diciembre).** Cheating in Online Assessment: Beyond Plagiarism. *Online Journal of Distance Learning Administration*, 3(2), State University of West Georgia, Distance Education Center. Retrieved from http://www.westga.edu/~distance/ojdla/summer72/rowe72.html
22 **Tapiador, M. & Singüenza, J. A. (2005).** *Tecnologías biométricas aplicadas a la seguridad*. México, D.F. : Alfaomega.
23 **Van Horn, Royal. (1998).** Data Mining For Research and Evaluation. *Phi-Delta-Kappan Technology Section*, 251-252.
24 **Varughese, J. (2005, abril).** Testing, Testing: Ensure the success of students with online assessment tools. Retrieved from http://www.universitybusiness.com/
25 **Weka (2005, 21 de diciembre).** Data Mining Software in Java. Retrieved from http://www.cs.waikato.ac.nz/ml/weka/
26 **Wisher, R., Curnow, C. & Belanich, J. (2005).** Verifying the Learner in distance learning. *18 Annual Conference on Distance Teaching and Learning*. Wisconsin, USA.

***José Alberto Hernández Aguilar.*** *He obtained his Doctorate degree on Engineering and Applied Sciences in November 2008 at Universidad Autonoma del Estado de Morelos (UAEM). Since November 2008, he is working as full time professor at the Sciences Faculty at UAEM. He is candidate to SNI. Areas of interest: Databases, Artificial Intelligence, On-line Assessment Systems, Marketing Research and e-commerce.*

***Gennadiy Burlak.*** *Worked in the Physics faculty at the National University of Kiev where he occupied several faculty positions- His last position was full-time professor at the Physics Faculty. Dr. G. Burlak entered to UAEM since 1998. He delivers several courses in the Physics and Computers areas. Nowadays he is SNI 2.*

***Bruno Lara*** *received his PhD from King's College, University of London in 2000 for research in Mechatronics. Since 2006 he is head of the computer science department in the Faculty of sciences of the Universidad Autonoma del Estado de Morelos. He is SNI 1. His main research interests include cognitive and evolutionary robotics, embodied cognition and in-vitro cell cultures.*