DEVELOPING A E-LEARNING MODEL FOR TRACKING THE CONTINUOUS ATTENDANCE OF THE STUDENTS

MOHSEN KHADEMI DEHNAVI [1] , SAYED MEHRAN SHARAFI [2] , NASER NEMATBAKHSH [3]
[1,2,3] Department of Computer, Islamic Azad University – Najafabad Branch, Esfahan, Iran
[1] khademi112@yahoo.com , [2] mehran_sharafi@iaun.ac.ir , [3] nemat@eng.ui.ac.ir

ABSTRACT

In the past decade, significant advances have been gained in e-learning systems; nonetheless, learning management systems are not free of difficulties. As the most important of these problems it can be pointed out that there is no guaranty whether the actual student is present in the virtual classroom or not and also there is no way to track the students' attendance continually during class time.

The main purpose of this paper is to present a new e-learning model based on web applications with attendance control ability. The presented multimodal biometric based model is used for identification, authentication and tracking the users. In this model two behavioral biometric characteristics (mouse movements and keystroke dynamics) and a physical one (face features) are used. A new algorithm is presented to demonstrate use of these three biometrics technologies. As the experiments' results show, in verification and attendance control processes the proposed solution needs a lower level of students' collaboration. After the implementation of this model it can be added to the existing LMS and become compatible with it. Therefore, this model can be used to track the continuous attendance of the users in sensitive stages of e-learning process.

Keywords: *E-learning, multimodal biometric, authentication, attendance, detection .*

1. INTRODUCTION

E-learning systems represent a new form of learning and are becoming more and more popular every day , therefore the need for security in this system is very sensible. Lack of adequate tools to properly track the users' behavior is one of the most important problems in learning management systems (LMS) [1,6]. Traditional solutions that recorded the interaction between the users and systems cannot guarantee that the user is who he or she claims to be and also they cannot find out whether the user is in front of the computer or not [4]. Information that is registered in the traditional users' log files just contains the students' entry and exit time. [1, 4]. A user could log in to the LMS then leave the system after a few minutes and return near the end of class only to log out. However, it is clear that this act is not reflected in the log files. There are many situations similar to the one described above where the traditional solutions can not specify the actual time duration the user spends in front of the computer.

This paper presents a multimodal biometric based solution to authenticate the users and control their attendance. Multimodal biometrics is useful in improving reliability of biometrics authentication when a single biometric authentication method cannot satisfy a required reliability level [3, 5, 9].

This paper is structured as follows: following this introduction, in section II related works are expressed. Section III express multimodal biometric. Proposed solution and biometrics technologies used in the model are discussed in section IV. System architecture is shown in section V. Section VI presents Implementation of Proposed solution. Experimental Result is shown in section VII. Finally, conclusion and future works are presented in the section IIV.

2. RELATED WORKS

There is much research on combining Biometric technologies in various fields including E-learning. Here are several of the most important researches related to this case: as reported in [8] details of the registered log files are combined with the biometric information obtained from users. These details contain: when the user starts working, the browser events and the browser focusing status. However, problems such as poor lighting conditions at students' room that can result in reduced performance of facial and iris verification methods. In addition, human factors can seriously reduce system performance. For

example: in facial verification, some users do not have appropriate positioning during most of class time for facial verification to work. Another solution is presented in [6] in a way that the system authenticates the users by the means of both facial features and fingerprint characteristics. As it is clear this system needs the users' collaboration, so continuous tracking with this method will cause interference for the users' activities. The fingerprints can easily be forged from touched surfaces, using a thin layer of gelatin or silicon.

In [3], student tracking is done only based on facial recognition. Although this can be done in 2 ways: collaborative and Non-collaborative and will lower the abuse probability, it also has its probable problems. For example, a student can put his image or video in front of the webcam and then leave the system.

Generally, if we want to use a system which contains just one biometric characteristic it would cause some problems that cannot be solved easily, so a Multimodal Biometric system consisting of three biometric characteristics is offered in this paper. These three are: facial features, keystroke dynamics and mouse movements. It is noteworthy that none of the past researches had focused on the combination of these three biometrics technologies mentioned in this paper.

3. MULTIMODAL BIOMETRICS

In this study, we tried to minimize the number of possible errors in authentication and tracking stages by combining several biometric characteristics of each user. This combination is performed by statistical or logical methods. The logical methods perform each authentication process in a separate manner and apply a logical AND or a logical OR on their results to get the final result. In statistical methods a multimodal authentication is done using each of the biometric characteristics and then statistical functions determine the final result [1, 5, 9, 13]. The reliability of the multimodal biometrics systems is evaluated using a density function for deceptive and honest users, along with false acceptance rate (FAR) and false rejection rates .

4. PROPOSED SOLUTION

In this proposed solution, a physical biometric system (face features) and two behavioral ones (mouse movements and keystroke dynamics) are used to authenticate, track and control the attendance of students. Attendance control system has been designed as a continuous monitoring system that collects the student's behavioral information during the learning sessions. This system is divided into three subsystems: (1) Face verification , (2) Mouse movements verification (3) , Keystroke dynamics verification. These subsystems are described in detail, in sections C to E sections.

4.1 Attendance Control Algorithm in E-learning

In this paper, we propose an algorithm to control the Attendance of students in virtual class which called ACT (Attendance Control Tracker) .To this end, ACT uses three biometric characteristics: facial features, keystroke dynamics and mouse movements. The ACT is designed in a way that any biometric characteristic can replace the ones used in this paper. The ACT expresses the process of attendance control and also describes the role of the mentioned biometric characteristics. The ACT performs in the following manner: In the first stage, to authenticate the students, their biometric data is received and then sent to the biometric authentication module on the server. In the next stage the authentication module compares this information with the user's pattern in the database and calculates the result as a numeric value. To get the authentication result, this number is compared with a threshold then if the result is positive the student can enter the virtual classroom. After the student's entry, his or her biometric information is continually sent to the Attendance controlling procedure. This procedure calculates the actual time that the student attended the virtual class and saves it in the student's records in the database. It also allows the instructor to access this information at the same time.

The ACT algorithm's steps are as follows:

Step 1. Registration: in this step, several patterns of the student's face, keystroke dynamics and mouse movements are received and stored in the system database.

Step 2. Biometric authentication: in every login, the authentication process is done by either only biometric methods or a combination of biometric characteristics with other methods.

Step 3. Attendance control using facial recognition: after the students' entry to the virtual class, they are tracked continually during the class and their facial features are compared with the information in the database. Any face detection has its own specified expiry time, for example n seconds, after n seconds elapse new face verification is needed.

Step 4. Attendance control using keyboard and

```
// Pseudo code for the ACT algorithm
Initialize:
Attendance =0 , Absence=0 ;
face-result=false ;
km-result=false ;
Collaborative-result =false ;
Timeclass=S // time of class is S seconds ;
While (Timeclass>0)
Compare face image with templates, get result in face-result ;
if face-result =false then
        Compare keystroke & mouse movement rhythm with
    template, get result in km-result ;
  end if
  if km-result =false then
        Collaborative verification by face, get result in
    Collaborative-result;
  end if
  if face-result=true or km-result =true or
    Collaborative-result=true then
        Attendance =Attendance +1 // Register a Attendance
    for student ;
  else
      Absence = Absence +1 // Register a Absence for student ;
  end if
  wait n seconds // n is expiry time for new verification ;
  Timeclass=Timeclass – n ;
end while ;
all-Attendance = Attendance × n ;
all-Absence = Absence × n ;
end // end of virtual class ;
```

mouse: behavioral information of mouse and keyboard is continually stored in the user's biometric files during his or her participation time in class and this information is used for tracking the student if captured images of the face are not suitable for facial recognition.

Figure 1 .Purposed Algorithm for Attendance control in virtual classes

Step 5.collaborative Attendance controlling: if the system cannot identify users using face images or mouse and keyboard information it will try collaborative verification. In this stage, the system will ask the user to put his or her face in an appropriate position and will take new images. At this stage, the user has a limited amount of time to do so and an expiry time will be determined.

Step 6. Measuring attendance rate: if the result of student's verification is positive the system will register an attendance mark for him or her otherwise he or she will be marked absent. At the end of the class, the overall time that the user has attended the class will be calculated using these marks.

It should be mentioned that the expiry time in the third and fifth steps depends on the following factors: network bandwidth, server or client processing power and the expected accuracy level. In an ideal situation expiry time is set by the instructor in order to determine the level of attention and order in the class. Pseudo code for the proposed algorithm is presented in Figure 1.

4.2 Decision making and combining methods

In the presented solution, simultaneous use of all three biometric subsystems is not essential and it is enough to just use the face detection subsystem in many situations. Tracking process based on facial features is started right after the student logs in and without his or her collaboration. As long as the user can be tracked using facial features, the raw data collected by the behavioral biometric subsystems are stored in the student's log files. The students' authentication and tracking processes are done using mouse movements and keystroke dynamics subsystems only if it is impossible for them to be done by the means of facial detection. Advantages of this method include reduced number of calculations for authenticating a user and Provide desirable reliability for the system.

In proposed model, if it is needed to authenticate the student by two mentioned behavioral biometric subsystems their authentication processes should be done independently and the final result will be obtained by applying a logical AND on their independent results. Acceptance or rejection of a student in this process is dependent on the system's policy.

4.3 Face recognition subsystem

The face recognition system is based on the viola-Jones algorithm [11,12,14]. The face authentication and tracking module has been developed using Matlab programming. This module uses a face detector and tracker to find and track the face of new users. With the user in sight the system detects his or her face and checks the positioning of the face. Face tracking continues for as long as the user is in sight and his or her face is not covered.

In this paper, face detection will be performed by "video-to-image" method. In this method, in the registration stage two video samples of the user are recorded and the authentication process in future

logins will be done by comparing an image with these two videos. In this method videos of the user are recorded during the registration stage in the following positions:

A. Reading a 200-word text.
B. Typing a text.

Figure 2 shows this tow Status. Each recoded video is three seconds long with number of frames depending on the frame rate of the webcam. The video frames of first case will be put in vector T_1 and second case video frames will be put in vector T_2. For tracking the user in the future logins, a three second video of the user will be recorded and its best frame in terms of face expressions, lighting and resolution will be selected by an application previously installed on the client part of the system, this frame is called V. This frame will be sent to the server side and there it will be compared with T_1 and T_2. The main strategy of comparing frame V with two pattern frames (T_1 and T_2) is to compare it with all of the frames in these two vectors. These comparisons will result in S_1 and S_2 value vectors.

Figure 2 .images of an individual in tow positions: 1) reading, 2) typing

For authenticating or tracking the user in the future logins, a three second video of the user will be recorded and its best frame in terms of face expressions, lighting and resolution will be selected by an application previously installed on the client part of the system, this frame is called V. This frame will be sent to the server side and there it will be compared with T_1 and T_2. The main strategy of comparing frame V with two pattern frames (T_1 and T_2) is to compare it with all of the frames in these two vectors. These comparisons will result in S_1 and S_2 value vectors:

$$S_A=\{S_{A1},S_{A2},\ldots,S_{AN}\} \quad (1)$$

$$S_B=\{S_{B1},S_{B2},\ldots,S_{BN}\} \quad (2)$$

In these two equations, S_{Ai} express the level of similarity between frames i and V. The final result of comparing T_1 and T_2 with V is calculated in the equation (3):

$$S_m= \max \{\max (S_A) , \max(S_B)\}$$
$$=\max\{\max\{ S_{A1},\ldots,S_{AN}\},\max\{ S_{B1},\ldots,S_{BN}\}\} \quad (3)$$

If S_m is higher than the specified threshold the result is positive otherwise it considered negative. The above mentioned threshold is determined according to the expected precision of the system, and it may vary.

4.4 Mouse movements pattern recognition subsystem

Mouse movement pattern is a signature that is extracted from mouse movements and other actions. Extracting mouse movement pattern doesn't need any special hardware; it can be done non-interactively during the entire class or at any particular time of class [7]. Mouse movements have many features that are extracted for use further analyses. The following items are some examples of these features: speed and acceleration of mouse pointer, mouse direction, amplitude of hand tremble, scroll wheel use, right and left click frequency and mouse idle time [7, 15].

The mouse pointer speed is the traversed distance by the pointer during a fixed period of time. The acceleration is calculated as the difference between the current speed and the speed measured during the previous time period. The hand tremble factor indicates the oscillation frequency of the mouse pointer.

Data collection is performed by the means of a hidden background sub procedure. When the user uses the mouse, the movement pattern and the time spent to use mouse are calculated in milliseconds, and saved in a database record specific to each user. Then the data are processed and displayed in various graphs. In order to model mouse movement, eight directions are considered. these directions are numbered from one to eight. Each of these eight directions, extending 45 degrees, covers a set of mouse movements. Suppose that user moves the mouse in the first sector (0 to 45 degrees). Average speed for the traversed distance is calculated. Altogether these pieces of information constitute the components of user's mouse movement pattern [7, 15].

4.5 Keystroke dynamics recognition subsystem

Keystroke dynamics is a behavioral biometric method that doesn't require any additional hardware to collect the information just as the mouse movement subsystem. To get the keystroke dynamics

pattern) the intervals between pressing the keys are calculated and considered as that person's signature. This method is based on the fact that each user has his or her personal keystroke dynamics signature. This method used in combination with other biometric methods plays a complementary role. The following factors are some keystroke dynamic features: the time that the key is held in pressing mode, key pressing intervals, total speed of typing etc. Sometimes it is necessary to record more than one pattern for each student because these patterns depend on keyboard's layouts, student's mood and work environments. There are various methods for analyzing keystroke dynamics; for example: fuzzy logic techniques, statistical methods and neural networks. As shown in [16] statistical methods have the highest accuracy level. Two main features that are considered as the result of students' actions are: (1) Key code: the ASCII code of each pressed key. (2) Pause duration between actions: this factor indicates the time interval between pressing two keys. This time interval is called a digraph. This factor depends on keyboard's layout and the hardware used to collect data [10,16]. Therefore; the main purpose of this strategy is to choose an architecture model, containing both software features and environmental factors which affect the user's moods to analyze keystroke dynamics. So, the following results are obtained:

let $R=(r_1, r_2, r_3, \dots, r_n)$ be a vector consisting of N digraphs generated when a user types an N+1 letter long word during the process of collecting the user's patterns. This set is called the reference vector. Let $U=(u_1, u_2, \dots, u_n)$ be another vector consisting of N digraphs generated when a user types an N+1 letter long word while being authenticated and tracked during the time that he or she is typing. This vector is called the test vector. These two vectors are compared taking into account certain criteria for which the explanation is outside the scope of this paper. These criteria are chosen so that they minimize FAR and FRR level which results more accuracy and less errors. This comparison results will be used in user identification.

5. SYSTEM ARCHITECTURE

As mentioned previously, this method will perform better in security, and adaptability (versatility) and processing power. The authentication and the attendance control module are two separate systems and are both server side programs. This system only requires a personal computer and a webcam. Thereupon the three above mentioned biometrics can be received from the user. The Proposed model is adaptable to Open Source CMS, so it can be added to these CMSs. Figure 3 shows architecture of the proposed model.

6. IMPLEMENTATION

In this paper, the control of access and attendance are performed using the BioWebAuth (Biometrics for Web Authentication) framework. BioWebAuth is an open source Java framework that is used for web-based authentication [2,15]. BioWebAuth presents a biometric-based access control mechanism and helps the Learning Management System (LMS) to authenticate the students and control their attendance. BioWebAuth allows us to

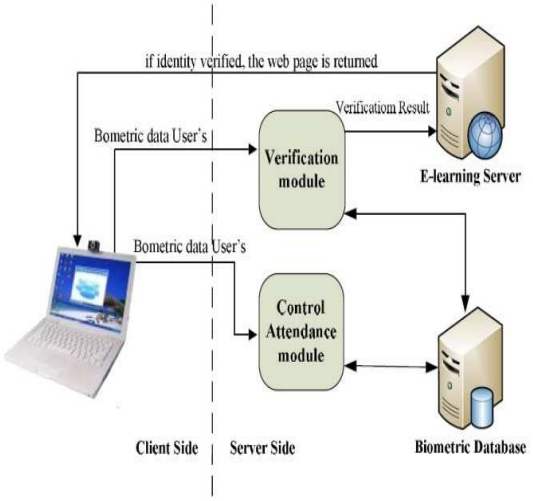

Figure *3 .Architecture* of the Proposed model

use a wide variety of biometric modalities combinations to control the students' access. In this paper, access control and student tracking are performed by BioWebAuth mechanisms. Our final choice for authentication and attendance control processes are two behavioral biometric patterns (mouse movements and keystroke dynamics) and a physical one (face features)[2,4].

Open source LMSs such as Moodle, ILIAS and Claroline are well-known web application programs which are able to authenticate through BioWebAuth. In this paper, Claroline and ILIAS systems are used to demonstrate the usability of the proposed developed system.

7. EXPERIMENTAL RESULTS

This model was developed in an experimental environment and an LMS, called Claroline, was used to test the proposed algorithm. Eight computer major students participated in an hour-long virtual class in a classroom equipped with Claroline. Each student had

a computer and a webcam attached to it. To evaluate the proposed method two three-second videos of each student were as face patterns and two other patterns was obtained by recording mouse movements and keystroke dynamics. The results of the proposed algorithm for a sixty-minute long class are presented in Table 1.

In this experiment, only one of the eight students needs multimodal biometric authentication. This rate is about 12.5 percents of all. While in the proposed solution presented in [5] about 18.5 percents of all users need multimodal biometric authentication. Adding the two mentioned behavioral biometrics (mouse movements and keystroke dynamics) in this solution reduces the need for multimodal biometric authentication by facial features. Thus in this model the user's comfort is increased. Another advantage of this proposed model compared with other solutions is that it does not need high bandwidth.

Table 1. Student attendance percentage in virtual class using the proposed solution

	Attendance rate with a threshold of 2%	Attendance rate with a threshold of 5%	Actual attendance rate
Student 1	95%	98%	100%
Student 2	99%	100%	100%
Student 3	97%	98%	100%
Student 4	96%	97%	100%
Student 5	68%	69%	70%
Student 6	79%	81%	82%
Student 7	54%	57%	60%
Student 8	8%	9%	10%

8. CONCLUSION AND FUTURE WORKS

By using the proposed model important tasks like controlling the student's attendance, student's evaluation and tracking are performed more accurately and also more completely. The proposed solution guarantees the student's attendance in front of the computer and his or her participation in the virtual class. However, the possibility of abuse is still probable by considering human factors. Nowadays perfect security can only be achieved by the means of human monitoring methods. As a future activity to improve the systems performance we can mention presenting a new model for controlling the students during an electronic test to minimize the misuses. In reaching this goal, the student's physical and behavioral information and also mental state should be monitored and processed.

REFERENCES

[1] Kornelije Rabuzin, Miroslav, Mario Sajko, "E-learning: Biometrics as a Security Factor", proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'06), IEEE, 2008.

[2] http://sourceforge.net/projects/biowebauth, Biometrics for Web Authentication (BioWebAuth) project.

[3] E. González, L.E. Anido, J.L. Alba, C. García. "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments" Proceedings of Eighth IEEE International Conference on Advanced Learning Technologies (ICALT '08), pp. 551-553, July 2008.

[4] E. González-Agulla, E. Argones-Rúa, C. García-Mateo, and Ó W. M.Flórez, "Development and Implementation of a Biometric Verification System for E-learning Platforms", EDUTECH, Computer-Aided Design Meets Computer-Aided Learning, IFIP 18th World Computer Congress, 2006, pp. 155-164.

[5] E. Gonz´alez Agulla ,E. Argones R´ua, J. Luis Alba Castro. " Multimodal Biometrics-based Student Attendance Measurement in Learning Management Systems". 11th IEEE International Symposium on Multimedia 2009.

[6] T. M. J. Auernheimer, B. "Biometric Authentication forWebBased Course Examinations". In HICSS, 2007.

[7] Ahmed Awad E. Ahmed and Issa Traore, "A New Biometric Technology Based on Mouse Dynamics" IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 3, pp 165-170, July-September 2007.

[8] J. L. Alba Castro, E. Gonz´alez Agulla, E. Argones R´ua,and L. Anido Rif´on. " Realistic measurement of student attendance in LMS using biometrics". In To appear on the Proceedings of the International Symposium on Engineering Education and Educational Technologies: EEET 2009,2009.

[9] L. Hong, A. K. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?", Proc. AutoID '99, pp.59-64, October 2005.

[10] I.Sogukpinar, L. Yalçin, "User identification via keystroke dynamics",Ist. Üniv. Journal of Electrical and Electronic Engineering, vol. 4, no. 1,2004, pp. 995-1005,2007.

[11] D. Gonz´alez-Jim´enez and J. Alba-Castro. "Shape-Driven Gabor Jets for Face Description and Authentication". IEEE Transactions on Information Forensics and Security,2(4):769–780, 2007.

[12] S. Sanderson and J. Erbetta, "Authentication for secure environments based on iris scanning technology", in IEEE Colloquium on Visual Biometrics, vol. 8, pp.1-7, 2005.

[13] Bharati, S.; Haseem, R.; Khan, R.; Ritzmann, M.;Wong, A. "Biometric Authentication System using the Dichotomy Model", Proc. CSIS Research Day, Pace Univ., May 2008.

[14] Chinese Academy of Sciences – Institute of Automation. Database of 756 Grayscale Face Images. Available: http://www.sinobiometrics.com, Version 1.0,2003.

[15] Seno, S. Sadakane, T. Baba, Y. Shikama, T. Koui, Y. Nakaya, N. - "A Network Authentication System

with Multi-Biometrics", IEEE, vol. 3, pp 914 – 918, September 2003.

[16] Haider, S.; Abbas, A.; Zaidi, A. "A Multi-Technique Approach for User Identification through Keystroke Dynamic"s, IEEE International Conference of Systems, Man and Cybernetics, Vol 2, 2004, pp. 1336-1341.