A FRAMEWORK OF SECURE BIOMETRIC BASED ONLINE EXAM AUTHENTICATION: AN ALTERNATIVE TO TRADITIONAL EXAM

T. Ramu, Dr.T. Arivoli

Abstract— In the past fifteen years the use of Internet technologies has been substantially growing for delivery of educational content and online learning has become increasingly popular and evolved. Online examination is an integral and vital component of online learning. Student assessment in online learning is largely submitted remotely without any face-to-face interaction and therefore, student authentication is widely seen as one of the major challenges in online examination. This study aims to investigate potential threats to student authentication in the online examinations and analyzing the benefits and limitations of the existing authentication approaches. Online examinations pose a unique problem, in that it can be very difficult to provide true user authentication. Due to the inherent anonymity of being online, compared to taking an examination in a classroom environment, students may attempt to artificially boost their scores in online examinations by having another individual take the exam for them, which a typical user/password authentication scheme cannot detect. For this purpose, we propose the Framework of Secured Biometric student authentication in Online Examinations. This framework uses a multi-modal authentication approach to secure online examination. The solution comprises of two layers of authentication i.e. student biometric authentication and Knowledge based authentication. In this paper, we propose a framework that provides security to improve on-line examination by utilizing technologies such as biometric authentication based Keystroke Dynamics. This paper attempts to address this important problem by proposing a theoretical framework that incorporates available biometric authentication technologies in conjunction with Knowledge based authentication. Discussions on future research and possible implications of the proposed theoretical framework for practice are provided.

Index Terms— Online Examination, Secure biometric Authentication, Keystroke dynamics

1 INTRODUCTION

In today's world learning capability is judged by means of examinations. Thus, the need of exams today in universities, schools, colleges and even companies for recruitment purposes. The general paper-pen tests/exams are now slowly being replaced by the online internet based testing system. The growth of Internet has largely evolved teaching and learning from a conventional class room into an invaluable educational resource accessible remotely from disperse geographical locations, beyond physical boundaries. The online learning environments are likely to be accessible, available, updatable, resource efficient, useable, economical [1] and have been widely adopted by a number of educational institutions in various disciplines.

The main advantage of online examination is that it can be conducted for remote candidates and evaluation of answers can be fully automated for MCQ questions and other essay type questions can be evaluated manually or through automated system, depending on the nature of the questions and the requirements. Also online examinations can be conducted at any time and does not incur higher cost as traditional exam scenario as there is no paper work involved (e.g., printing ex -am papers, prepare paper admissions etc.,) , there are no invigilators, also no need of arrangement of exam centers. When comparing with traditional exam scenario the cost for an online examination will be almost zero. In the online learning, examination is integrated with the teaching and learning components. In an online examination scenario, there may be no face to-face interaction between students, tutors and administrators [2], thus, security is vital to the credibility of online learning environments. The nature of online learning environments makes it more vulnerable to various security threats. Online examinations being an integral part of the learning environment can be high stake applications, which may fall to impersonation and malicious attacks for higher grades [3]. One of the primary goals of student authentication is to ensure the genuine interaction of individual students with the online examination. The conventional user-id and password authentication is not sufficient to verify the identity of an online student.

Online exam has expanded rapidly [4], [5]. Even though, the offline exam is usually chosen as evaluation method for both on-line and off-line exams. Online course examinations are useful to evaluate the student's knowledge using modern computer technology without any effects on the traditional university course exam that uses Pens, Papers and invigilators. Online exam can improve the standards of student's examina-

- *T..Ramu is currently pursuing PhD program in Kalasalingam University, India. E-mail: loginworld34@hotmail.com*
- *Dr.T .Arivoli is currently working as professor in vickram engineering college,India. E-mail: t_arivoli@gmail.com*

tion whereas the traditional examination system using the pen and paper requires more effort on the part of students and invigilators. Online examinations are considered an important source for university exam, and the development of network technology polices has given the possibility to conduct the exams online. Thus, the university students can benefit from these services. University course exams , using the multiple choice questions and allowing the students to choose only one answer from alternative answers or the true/false questions, are traditionally using the paper and pens and they have always been a heavy load for both students and lecturers. Computer new technology has been generally useful to the fields of education. In attitude and tools, the new computer technology gives the lecturer the advantage of an effective assessment. The traditional way of identifying the students is checking the student card, driving license, resident card or Passport.

The online process and security of the online exam system helps with eliminating cheating. This paper proposes the usage of biometrics which supports the security control, authentication and integrity of online exam process. E-monitoring of students uses finger prints and cameras for preventing cheating and substitution of the original student. This paper targets the online exam for basic computer in university courses with students at particular locations, at a fixed time and jumbled questions for all examinees at the restricted physical location of the examinees.

Most modern online education uses Web-based commercial courses management software [6] such as Web CT [7], blackboard [8], or software developed in-house. This software is not used widely for online exams, due to security vulnerabilities, and the system must rely on students' honesty or their having an honor code [9]. A study has been conducted on online exam and traditional exam which indicates that an online exam has better results than traditional exams. [10]

This paper discusses existing authentication features, and reviews their benefits and constraints. We have designed and developed a biometric Authentication Framework (BAF) for online examination. In section 2 discussing about the potential threat of online examination and section 3 , we review various authentication methods of online examination. Section 4, we review various biometric authentication and section 5 present the framework of secure online examination and section 6 discuss on future research and possible implications of the proposed theoretical framework for practice are provided.

2 Potential Threat

The online examination approach essentially differs from the conventional face-to-face examination. In the online learning environments, technology is harnessed with assessment techniques to assess learning outcomes. Online examination is a fundamental and integral part of the learning environment. The online examinations may include questionnaires, assignments, projects, peer review, essays, quizzes, self-assessment and portfolios [11]. In the online learning and examination, students interact and submit their work remotely and therefore, building confidence and trust is of vital importance [12]. The online teaching and learning approaches has largely changed student assessment methods. The two different assessment approaches used in the online environments, are summative and formative assessments

In the summative assessments, student's learning outcomes are evaluated and their skills are measured against the learning goals using various assessment techniques. In online examinations, summative assessment may be at greater risk of attack due to its high-stakes. Tutors typically use formative assessment to review feedback on learner's activities [13] and record progression. Formative assessment does not count towards final result or grades and this characteristic is likely to reduce security threat in online learning environments.

In spite of the anticipated benefits of online learning, security remains one of the major issues and a threat to the success of online learning [14]. As in [15], online learning offers more opportunities for academic dishonesty from remote locations than traditional face-to-face learning and assessment. Lin [16] suggests that academic dishonesty has always been one of the challenges of higher education and cheating and academic dishonesty is an ongoing issue. Academic dishonesty ranges from cheating in examination session to plagiarism or originality of work submitted.

Plagiarism: Plagiarism is seen as one of the major challenges to both online and face-to-face examination. In plagiarism, students imitate or appropriate someone else's original idea or scholarly work and claim to be the original author. The students submit the plagiarized work as part of their assessment. Evidence suggests that plagiarism is on the rise [17] and it can be a potential treat equally to both online and face-to-face learning and examination. A large number of plagiarism detection software's are employed to check originality of the submitted work. Plagiarism can be one of the potential challenges to online learning; however, our research mainly focuses on student authentication in online examination.

Cheating: In online examinations, the students submit their work remotely and it poses a challenge to verify the identity of a person taking online examination as the same person who registered and completed the course work [18]. Cheating and student impersonation have been a serious problem to the reputation of online learning. Agulla [18] identifies the rise in academic dishonesty in online examinations to gain maximum marks as a threat to online learning. The threat level is higher for online systems because it has increased the opportunities for deception due to non-rigorous authentication regime. As in [19], unethical conducts have intensified in online learning due to more opportunities for cheating in online examination as a result of use of technology and the Internet.

3 Authentication Method

Reliable student authentication is extremely relevant to online examinations because of high stakes being involved. Authentication attempts to verify that the users are who they claim to be. In an online examination scenario, authentication aims to verify the identity of online students and plays a key role in security. Unlike face-to-face (traditional) examinations, authentication in online examinations is not supervised and in-

vigilation is largely different in an uncontrolled remote environment [20]. Authentication guarantees the currency of online examinations, as the legitimate interaction between a student and the online examination is more likely to lead to authentic results. The mainstream authentication techniques are based on user's knowledge, objects possession and biometric features. The method of various authentications in online examination is shown in figure 2.

3.1 Knowledge Based Authentication

As in [20], knowledge based authentication verifies Identity on the basis of "what you know". It requires personal knowledge to authenticate individual access to the online environment. A user-id and password scheme is a commonly used example. It is a popular authentication method, because passwords are key to authentication and memorable. In a scenario like banking, where users are highly likely to make every effort to prevent illicit access, this scheme can be effective. However, due to the nature of online examinations, students may conveniently share their login credentials with a third party to boost their grades. As analyzed in [21], low entropy passwords are prone to dictionary attacks. Hence, online examinations relying on a user-id and password are susceptible to collusion and malicious attacks.

Challenge questions or security questions are another example of knowledge based authentication. It is generally used in the banking sector [22] for authentication, and corporate email service providers for credential recovery [23].

3.2 Object Based Authentication

In the object based authentication, individuals in possession of identity objects are believed to be authentic. The users are identified by presenting or applying physical objects i.e. electronic chip cards, magnetic cards, RFID tag and digital keys. It is broadly used in the banking sector, transportation and secure premises access. The identity objects such as electronic and magnetic cards benefit from storage of individual's identification features. In an online examination scenario, the presence of both entities i.e. identity object and student, increases the security. However, objects may be transferred to a third party or compromised, which poses potential threat to the online examinations [24] e.g. collusion. In addition, it may require special purpose devices to take user input for registration and authentication.

3.3 Profile Based Authentication

In [25], Profile Based Authentication for student authentication in online examinations. This authentication possess i.e. user-id and password, and challenge questions. Initially, a user-id and password can be used to login into the online learning environment to carry out regular learning activities. During the learning process, students are posed with profile questions that are used to extend and refine individual student's profile. When a student requests to access an online examination, the second layer of authentication triggers the challenge questions, which are generated from the student's profile. The profile questions are used to collect answers in order to build and update the student's profile. Challenge questions are used to verify the student's identity. The primary focus of the proposed solution is secure authentication for online examination. The profile is a student's description in the form of questions and related answers. It represents a student by using information received from questions and answers during registration and learning process. The questions and answers in a student profile can pertain to personal information, education, activities, professional experience, hobbies, future objectives, and learning activities. In the authentication process, if the collection of answers to profile questions and answers to challenge questions matched the stored authentication results then student is granted access to online examination. If the answers to challenge question do not match to the stored profile information, student is denied access. Due to the nature of online examinations, students may conveniently share their login credentials and profile information with a third party to boost their grades.

4 BIOMETRICS BASED AUTHENTICATION

Biometrics is defined as the identification of an individual based on physiological and behavioral characteristics. Commonly used physiological characteristics include face , hand (fingerprint, hand geometry, palmprint), eye (iris and retina), ear, skin, odor, dental, and DNA. Commonly used behavioral characteristics include voice, gait, keystroke, signature, mouse movement, and pulse. Two or more of the aforementioned biometrics can be combined (Multimodal) in a system to improve the recognition accuracy. In addition, some soft biometric traits like gender, age, height, weight, ethnicity, and eye color can also be used to assist in identification. Rabuzin et al. [26] and Asha et al.[27] proposed to combine several different biometric traits in the field of e-learning.

The biometrics authentication is performed by the verification of an individual's physical or behavioural characteristics [28]. Biometric frees individuals to memorize passwords and carry cards, as the person is the key for identification [29]. A number of biometric authentication features have been evolved from recent research and implemented in online learning systems including finger print, video authentication, face recognition, audio recognition or combination of these features in the form of multi-modal biometrics.

Generally a biometric system is designed to solve a matching problem through the live measurements of human body features. It operates with two stages. First, a person must register a biometric in a system where biometric templates will be stored. Second, the person must provide the same biometric for new measurements. The output of the new measurements will be processed with the same algorithms as those used at registration and then compared to the stored template. If the similarity is greater than a system-defined threshold, the verification is successful otherwise it will be considered unsuccessful. Due to the fuzzy measurements of biometrics error correction coding is needed. Table 1 lists a few biometrics and their features for authentication with error correction.

4.1. Fingerprint Authentication

Ramin [30] proposed approach that can incorporate a random fingerprint biometrics user authentication during exam taking in e-learning courses. Alotaibi [31] also proposed using fingerprints for E-exams. Fingerprint is one of the most commonly used biometrics authentication features [32], which offers a unique global identifier. The fingerprint may offer secure solution and minimize threat of impersonation in online examinations. The wider implementation of fingerprint for online examination requires additional resources i.e. fingerprint scanners and software on the client's location.

4.2 Face Authentication

Penteado and Marana [33] proposed to use face images captured on-line by a webcam in Internet environment to confirm the presence of users throughout the course attendance in an educational distance course. Face recognition biometric trait implements image recognition and pattern matching algorithms to verify user identity [34]. It may be a reliable authentication candidate for online examinations. However, face recognition biometric may not be secure authentication for online learning system due to the complexity of face recognition technology [3]. Various aspects such as variable face expression capture point direction, variable light, environment, web camera, weather and other pertinent accessories e.g. beard, glasses can affect the authentication results.

4.3 Voice Authentication

The audio or voice biometric is used both for speech recognition and speaker identification. In this biometric trait, human voice is recognized using automated system based on the data from speech wave. As in [2], intra-individual variations i.e. human voice features like acoustic, voice pitch and speaking style or accent provide a unique identifier for use as a biometric feature. As a behavioural authentication technique, it may be a secure option to shield online examinations. However, varying speaking speed, environmental noises, quality of recording equipment's may not result in robust outcome [35]. The intra-individual variation can be a major practical issue in voice recognition. In the context of online learning, user training can be an overhead, when recording voice samples during the enrolment and authentication phase. A user's voice may be recorded for use in replay attacks as the 'liveness' of the user cannot be verified [36].

4.4 Signature Authentication

Signature verification is a legacy feature and it has been widely used and highly acceptable in day to day life transactions [37]. However, as in [38], the evolution of technology has enabled the capture and verification of human signature using a combination of computer software and hardware. It is a unique behavioural trait and a potential candidate for user authentication. Purpose built accessories like digital signature pads, tablets and digital pens are used to capture signature information [39]. Unlike some biometric features, signature may not be easily replayed as only the signatory can reproduce the original signatures. However, signature recognition may face other issues i.e. complexities of algorithms, variation in signatures on different occasions, individual's emotional and physical influence on signature and signature forgery [40].

4.5 Keystroke Authentication

Flior et al. [41] presents a method for providing continuous biometric user authentication in online examinations via keystroke dynamics. Keystroke dynamics biometrics is a data processing technique that analyzes the way a user types by monitoring the keyboard inputs in attempt to identify them by their habitual typing patterns [42]. As compared to other physical and behavioral biometrics, keystroke dynamics biometrics falls short to be a sole biometrics authenticator. Conversely, by integrating keystroke dynamics biometrics into the existing password authentication system, even if the impostor is able to present the correct login information, either by hacking, key logger or shoulder spoofing, without the right typing pattern, they will be denied access. In contrast, sole password authentication will guarantee access to any user as long as the login credential received is correct not considering if the user is legitimate.

Most research works done by far were focusing on extracting keystroke timing latency as feature data and mainly focused on one or two types of keystroke features at a time. For example [43] proposed a simple statistical method in which duration of each key press and the time duration between each different key press were considered. The experimental result recorded an unfavorable FRR of 24%. The author asserted that the poor performance was partly caused by the poor typing skill of the users involved.

Monrose et al. [44] stressed that keystroke recognition based on fixed-text was more desirable than free-text. This was due to contributing factors such as uncontrolled environmental parameters, unconstrained inputs, and uncooperative user which imposed restriction on the usage of free-text recognition. The author used Euclidean distance and Bayesian alike classifier as the classification techniques in their study. The keystroke features extracted were keystroke duration and keystroke latency (time between a key is released and the next key is pressed). However, the performance result presented was not complete as the result only reported in FRR of 16.78% and 7.83% for Euclidean distance and Bayesian classifier respectively.

While most research works on keystroke dynamics have been conducted on conventional timing-based typing characteristics, [45] looked into the prospect of using typing pressure as keystroke feature. A conventional keyboard was customized into a pressure sensitive version by inserting special force detection sensors underneath the keyboard matrix. ARTMAP-FD neural network was used for keystroke pattern classification. They fed the network with keystroke pressure, keystroke latency, as well as the combination of both. The performances of the classifier using different sets of aforementioned keystroke features were recorded at an EER of 16.50%, 14.94%, and 11.78% respectively. Although the inclusion of keystroke pressure feature showed improvement in performance, the error

rate was still higher than the other traditional keystroke features based methods. Furthermore the practicability of such customized keyboard in large scale implementation was called into question due to limited availability.

Keystroke, two events occur each time the user types a character on the keyboard, to be precise ''key press" and ''key release". Each key event will be associated with a timestamp and this timestamp is the core component of the template generation process. Keystroke features can be extracted in terms of Dwell Time (DT), Flight Time (FT) , Difficulties of typing phrase ,Pressure of keystroke ,Typing rate ,Linguistic style ,Sound of typing Frequency of word errors.

Nevertheless, not all of the above features are favorable. For example, in order to acquire keystroke pressure feature, dedicated pressure sensitive keyboard is essential, which contradicts with the main advantage of keystroke dynamics biometrics. Frequency of word errors, typing rate, and difficulties of typing phrase are merely practical for text with large number of characters. Where else, there is a high concern with the noise associates with the acquisition devices used to record sound of typing.Dwell Time DT (also known as keystroke press time or hold time) is the time difference between a key press and key release of the same key and Flight Time FT (also known as keystroke latency) is the time interval between two successive keys press or release., timing interval between keystroke actions of different keys (also known as latency). Eventually, if we try to break down flight time further; we notice that it can be sub divided into three types (D2, D3, and D4) as in Figure 1. Explanation and method of calculation for each of these keystroke features based on example are given as follow.

Dwell Time (D1): The time interval between a key pressed until the key is released.

$$D1 = R1 - P1$$

Flight Time (D2): The time interval between a key press and the next key press.

$$D2 = P2 - P1$$

Flight Time (D3): The time interval between a key release and the next key press. Negative value may occur if the next key is pressed before the previous key release.

$$D3 = P2 - R1$$

Flight Time (D4): The time interval between a key release and the next key release.

$$D4 = R2 - R1$$

Template generation is the stage where user's keystroke feature samples are combined and transformed into a compact yet representative form. These templates are then stored in database for future authentication and retraining use. A user keystroke template is kept in the following format:

$$[\mu],[\sigma],[n]\sum_{i=1}^{n} t_{i^2}$$

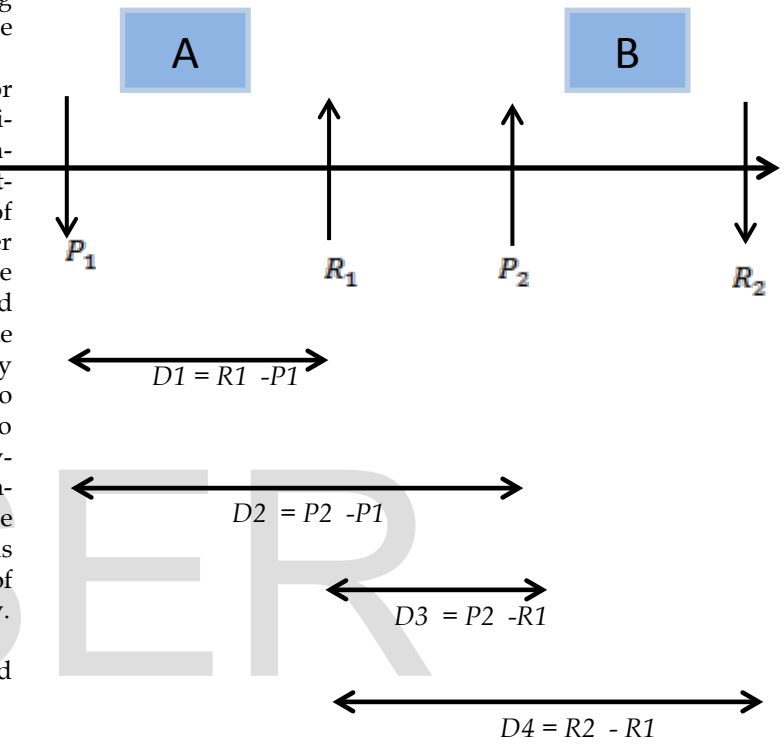


Figure 1: An example of four keystroke features using the phrase "AB".

where t represents the value of each latency, n is the number of training samples, while μ and σ is the mean and standard deviation of a particular set of latency.Gaussian probability density function (GPD) is used to compute the similarity score between a reference template and a test data template. The output score of GPD has the range of [0,1]. The nearer the score towards the value of one, the higher the similarity between the two tested templates. In other words the more likely the test data template belongs to a genuine user, and vice versa. Generally Gaussian function has the form of

$$S_{GPD} = \frac{\sum_{I=1}^{K} e^{-\left(\frac{(t_i-\mu_i)^2}{2\sigma^2}\right)}}{k}$$

TABLE1: BIOMETRIC FEATURES FOR AUTHENTICATION WITH ERROR CORRECTION METHOD.

Biometrics	Feature Extraction	Error Correction

Keystroke [5]	Duration, latency: durations for each letter typed and latencies between keystrokes	Discretization
Voice [6]	Text-dependent or text-independent speaker utterance units	Discretization
Signature [7]	Pen-down time, forward and backward time,pressure and Height to width ratio	Averaging
Face [8]	Facial features: positions, sizes, Angles	RS code
Iris [9]	Digital representation of iris image processed with Gabor wavelet	RS code / Hadamard
Fingerprint [10]	Minutiae points: ridge ending and ridge bifurcation	Quantization
Palmprint [11]	principal lines, wrinkles, minutiae, delta points	RS code

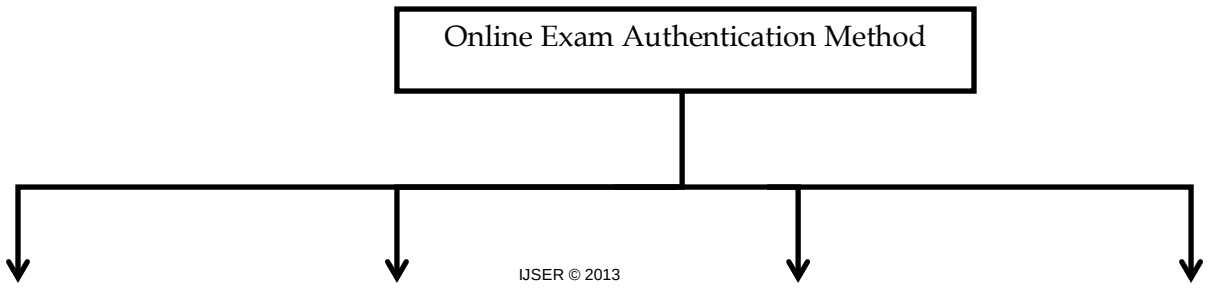
where S_{GPD} is the GPD score, t is the test data's latency of a particular character, k is the total number of keystroke feature in a phrase, μ and σ are the mean and standard deviation of a reference template, respectively. The formula indicates that the matching is performed on every latency in a phrase, which will yield separate individual sub score for each measurement. The final score is obtained by computing the average of all sub scores.Keystroke authentication to prevent students taking online exams from e-cheating and attempted to answer the question whether they have helped to achieve the goal of eliminating student dishonesty in online examination.Biometric authentication has its strengths and limitations in terms of usability, cost and security when used in online examinations. It aims to ensure the presence of individual students by verifying physical and behavioural characteristics, which can be a preferred way to counter impersonation. However, it may incur additional cost for using special purpose hardware and software kits, and its wider implementation globally could be a challenge. Unlike knowledge based authentication, the biometric features are not amendable and hence not useable if compromised. Some biometric features may require student training and additional administration to facilitate and monitor various processes. The outcome of the biometric authentication may be affected by variation in human physical and environmental atmosphere, reducing authentication accuracy.

5 PROPOSED FRAMEWORK

The figure 3 shows the proposed framework of secured biometric authentication in Online Examination. A framework uses a multi-modal authentication approach to secure online examination. The solution comprises of two layers of authentication i.e. student biometric authentication using keystroke dynamics and Knowledge based authentication. It shows the series of steps of online exam starting with the secured login using biometrics and system login through server till the end of exam results. The special exam group is created by grouping the hostnames / IP of clients for a specific location (Computer Lab) and time. To avoid the malpractice in the exams we use keystroke dynamics as a means to log into the exam and continuous evaluation. The user after identified login into the system uses the user-id and password provided by the university, which are authenticated by the server. This gives him/her permission to open the exam from the server otherwise the students cannot login into the system. The unauthorized users attempting to log into the system from remote computers are blocked by the proposed system Once the session begins the timer is on, the student completes his exam within the allocated time and once the time is up the system send an alert and logs the user off. The following steps are describing the proposed framework

Step 1: Student Identification: The system will check the identity of the student by using keystroke dynamics biometrics before entering the exam. This will also check whether the student is eligible for that particular exam.

Step 2: Exam Domain Login: The student will log into the exam domain of the university with the user name and password and profile information provided by the university domain login. If the user name and password and profile information are correct, then the user will be able to log into the exam.



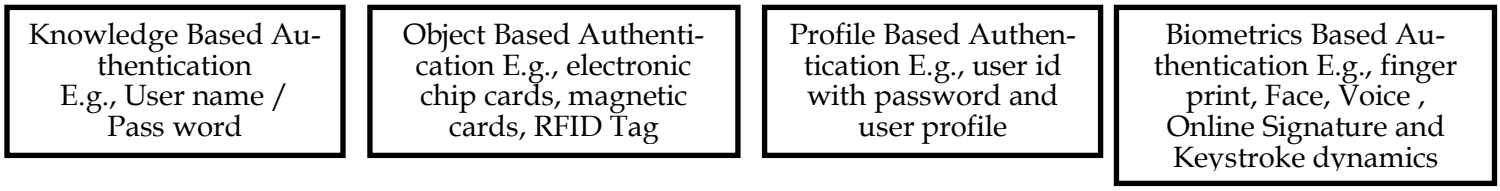


Figure 2: Types of Authentication methods in Online Examination

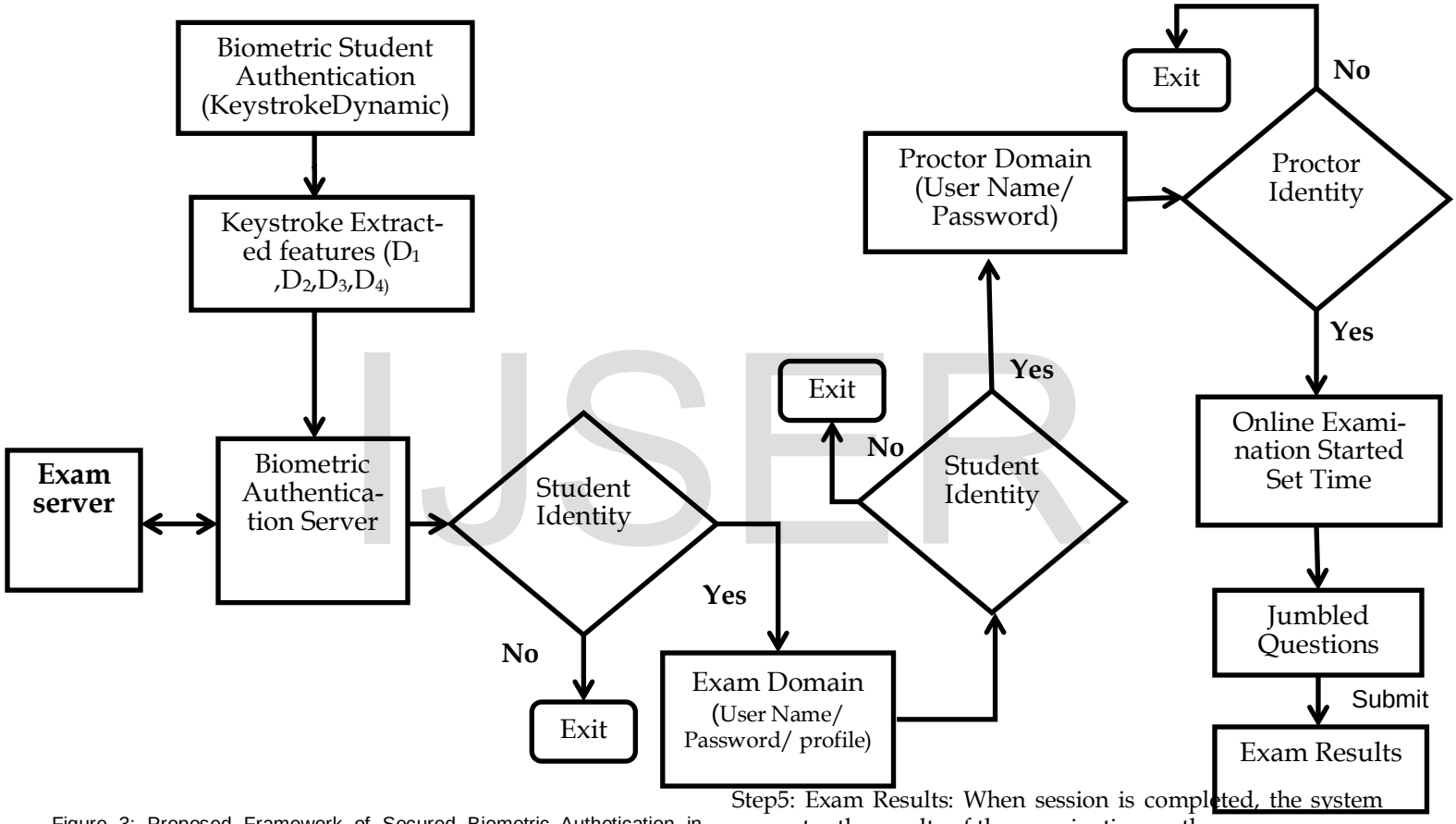


Figure 3: Proposed Framework of Secured Biometric Authetication in Online Examination

Step 3: Online Exam Proctor (Supervisor) Password: The supervisor password is given to the students who are successfully logged into the exam domain. This gives them access to the exam and the exam session begins for that specific exam.

Step 4: Random questions: The random questions are given to the students, who submit the answers to the server.

Step5: Exam Results: When session is completed, the system generates the results of the examination on the screen.

6 CONCLUSION AND RECOMMENDATIONS FOR FUTURE RESEARCH

Keystroke biometrics is the additional security mechanism which is invisible to users as they only need to type on a keyboard as usual, instead of providing their physical biometric data (i.e. fingerprint, iris image), where some users may feel uncomfortable. The security mechanism will be responsible to capture and process the users' typing timing patterns without their knowledge. Ease of incorporation into the existing password based authentication system and no additional device requirement increase the potential of keystroke dynamics to be deployed in real world application, such as online examination, online banking and password based security system.The popularity and growth of online learning has also led to an increased concern about security of online examinations. The

threats to online examinations can have a detrimental impact on the credibility of online learning courses that make extensive use of online examinations.

Conventional approaches to student authentication are unlikely to be sufficient to counteract collusion and malicious attacks to online examinations. We believe the online format is considerably superior to paper-and-pencil exams. This paper reviewed various authentications traits, their feasibility in the online learning environments, and their strengths to deal with collusion and malicious attacks. This paper proposed new framework and the findings from the empirical study reported here suggest, that keystroke based authentication with knowledge based authentication can be an effective technique. We have come to the conclusion that the secure online examination can be solved by using keystroke dynamics with additional knowledge based authentication. Future work would therefore, concentrate on the usability, security, privacy and reliability aspect of the keystroke authentication in online examination.

REFERENCES

[1] Ruiz J. G., Mintzer M. J., Leipzig R. M.,"The impact of e-learning in medical education", Academic medicine, 2006,81(3),207.

[2] Hayes B., Ringwood J. "Authenticating student work in an e- learning programme via speaker recognition", 3rd International Conference on Signals, Circuits and Systems (SCS) 2009, IEEE.

[3] Agulla E. G., Rifón L. A., Castro J. L. A., Mateo C. G. "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments", Eighth IEEE International Conference on Advanced Learning Technologies, 2008, IEEE.

[4] IC3 "Online". Available: http://www.ucertify.com/certifications//ic3.html

[5] The WebCT, SIMON FRASER UNIVERSITY "Online" available: https://webct.sfu.ca/webct/entryPageIns.dowebct

[6] J. C. Adams and A. A. Armstrong, "A Web-based testing: A study in insecurity," World Wide Web, vol. 1, no. 4, pp. 193–208, 1998.

[7] C. Rogers, "Faculty perceptions about e-cheating during online testing," J. Comput. Sci. Colleges, vol.22, no. 2, pp. 206-212, 2006.

[8] The Blackboard Northern Illinois Univ. [Online]. Available: http://www.blackboard.niu.edu/blackboard/

[9] C Adams and A. A. Armstrong, "A Web-based testing: A study in interesting," World Wide Web, vol. 1, no. 4, pp. 193-208, 1998.

[10] Eros Desouza, Matthew Fleming, "A Comparison of In-Class and Online Quizzes on Student Exam Performance", Journal of Computing in Higher Education, Vol. 14(2), pp. 121-134, spring 2003.

[11] Joosten-Ten Brinke D., Van Bruggen J., Hermans H., Burgers J., Giesbers B., Koper R., et al.,"Modeling assessment for re-use of traditional and new types of assessment", Computers in Human Behavior, 2007,23(6),2721-41.

[12] Karvonen K. "Creating trust", In Proceedings of the Fourth Nordic Workshop on Secure IT Systems, 1999, Citeseer.

[13] Birenbaum M.,"Assessment 2000: Towards a pluralistic approach to assessment", Alternatives in assessment of achievements, learning processes and prior knowledge, 1996,3-29.

[14] Alwi N. H. M., Fan I. S.,"Threats analysis for e-learning", International Journal of Technology Enhanced Learning, 2010,2(4),358-71.

[15] Jung I. Y., Yeom H. Y.,"Enhanced security for online exams using group cryptography", IEEE Transactions on Education, 2009,52(3),340-9.

[16] Lin C. H. S., Wen L. Y. M.,"Academic dishonesty in higher education—a nationwide study in Taiwan", Higher Education, 2007,54(1),85-97.

[17] Born A. D.,"How to reduce plagiarism", Journal of Information Systems Education, 2003,14(3),223-4.

[18] Agulla E. G., Rifón L. A., Castro J. L. A., Mateo C. G. "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments", Eighth IEEE International Conference on Advanced Learning Technologies, 2008, IEEE.

[19] [Harmon O. R., Lambrinos J., Buffolino J.,"Assessment design and cheating risk in online instruction", Online Journal of Distance Learning Administration, 2010,13(3).

[20] Moini A., Madni A. M.,"Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective", IEEE Systems Journal, 2009,3(4),469-76.

[21] Huiping J. "Strong password authentication protocols", 4th International Conference on Distance Learning and Education (ICDLE), 2010, IEEE.

[22] Rabkin A. "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook", In SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, 23, New York, NY, USA, ACM

[23] Schechter S., Brush A. J. B., Egelman S. "It's No Secret. Measuring the Security and Reliability of Authentication via", 30th IEEE Symposium on Security and Privacy, 2009, IEEE.

[24] Apampa K. M., Wills G., Argles D. "An approach to presence verification in summative e-assessment security", International Conference on Information Society (i-Society 2010), 2010, IEEE.

[25] Ullah A., Xiao H., Lilley M. "Profile Based Student Authentication in Online Examination", International Conference on Information Society (i-Society 2012), 2012, IEEE.

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

[27] S. Asha and C. Chellappan. Authentication of e-learners using multimodal biometric technology. International Symposium on Biometrics and Security Technologies, pp. 1-6, Islamabad (23-24 April, 2008).

[28] Asha S., Chellappan C. "Authentication of e-learners using multimodal biometric technology", International Symposium on Biometrics and Security Technologies 2008, IEEE.

[29] Gil C., Castro M., Wyne M. "Identification in web evaluation in learning management system by fingerprint identification system", Frontiers in Education Conference (FIE), 2010, IEEE

[30] Yair Levy and Michelle M. Ramin. A Theoretical Approach for Biometrics Authentication of e-Exams. Available at: http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

[31] S. Alotaibi. Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. The 4th Saudi International Conference, The University of Manchester, UK (July 2010).

[32] Aggarwal G., Ratha N., Jea T. Y., Bolle R. "Gradient based Textural Characterization of Fingerprints", Biometrics: Theory, Applications and Systems, 2008, IEEE.

[33] Bruno E. Penteado and Aparecido N. Marana (2009). A Video-Based Biometric Authentication for e-Learning Web Applications. Enterprise Information Systems. Lecture Notes in Business Information Processing, 24(IV): 770-779.

[34] Zhao Q., Ye M. "The application and implementation of face recognition in authentication system for distance education", 2nd International Conference on Networking and Digital Society (ICNDS), 2010, IEEE.

[35] Shaver C. D., Acken J. "Effects of equipment variation on speaker recognition error rates", International Conference on Acoustics Speech and Signal Pro-

cessing (ICASSP), 2009, IEEE.

[36] Eveno N., Besacier L. "Co-inertia analysis for liveness test in audio-visual biometrics", Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, 2005, IEEE.

[37] Adamski M., Saeed K. "Online Signature Classification and its Verification System", 7th Computer Information Systems and Industrial Management Applications2008, p. 189-94.

[38] Meshoul S., Batouche M. "Combining Fisher Discriminant Analysis and probabilistic neural network for effective on-line signature recognition", 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), 2010, IEEE.

[39] S. Asha and C. Chellappan. Authentication of e-learners using multimodal biometric technology. International Symposium on Biometrics and Security Technologies, pp. 1-6, Islamabad (23-24 April, 2008).

[40] Jazahanim K. S., Ibrahim Z., Mohamed A. "Online zones' identification using signature baseline", Second International Conference on the Applications of Digital Information and Web Technologies, 2009, IEEE.

[41] Eric Flior, and Kazimierz Kowalski. Continuous Biometric User Authentication in Online Examinations, pp.488-492. Seventh International Conference on Information Technology (2010).

[42] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabuuti, "User authentication through typing biometrics features," in Biometric Authentication, Proceedings, vol. 3072, 2004, pp. 694–700.

[43] D. C. D'Souza, "Typing Dynamics Biometric Authentication," University of Queensland, Queensland, 2002.

[44] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," Future Gener. Comput. Syst., vol. 16, no. 4, pp. 351–359, 2000.

[45] C. C. Loy, W. K. Lai, and C. P. Lim, "Keystroke Patterns Classification Using the ARTMAP-FD Neural Network," in Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on, 2007, vol. 1, pp. 61 –64.

[46] F. Monrose, M. Reiter, and S. Wetzel (1999). Password Hardening Based on Keystroke Dynamics. Proc. of the ACM Conference in Computer and Communications Security, pp: 73– 82.

[47] F. Monrose, M. Reiter, Q. Li, and S. Wetzel (2001). Cryptographic key generation from voice. Proc. of the IEEE Symposium on Security and Privacy.

[48] F. Hao, and C. Chan (2002). Private key generation from on-line handwritten signatures. Information Management & Computer Security, 10(2): 159–164.

[49] B. Chen, and V. Chandran (2007). Biometric Based Cryptographic Key Generation from Faces. Proc. of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Application, pp: 394 – 401.

[50] F. Hao, R. Anderson, and J. Daugman (2005). Combining cryptography with biometrics effectively. Technical Reports, University of Cambridge, Computer Laboratory.

[51] U. Uludag, S. Pankanti, and A. Jain (2005). Fuzzy Vault for Fingerprints. Proc. of Audio and Video-based Biometric Person Authentication, pp: 310-319.

[52] A. Kumar, and A. Kumar, A. (2008). A palmprint-based cryptosystem using double encryption. Proc. of SPIE,6944:1-9.