Student Cheating Detection System in E-exams

By Razan Hamza Bawarith

A thesis submitted for the requirements of the degree of Master of Computer Science

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
KING ABDULAZIZ UNIVERSITY- JEDDAH
Shaaban 1438H – May 2017G


بسم الله الرحمن الرحيم

بـــــسم الله الرحـــــمن الرحـــــيم

﴿ وَمَا تَوْفِيقِي إِلا بِاللهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ ﴾ **سورة هود: آية 88**

Student Cheating Detection System in E-exams

By Razan Hamza Bawarith

A thesis submitted for the requirements of the degree of Master of Computer Science

Supervised By

Dr. Abdullah Basuhail
Dr. Anas Fattouh
Prof. Dr. Shehab Gamalel-Din

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
KING ABDULAZIZ UNIVERSITY
JEDDAH – SAUDI ARABIA
Shaaban 1438H – May 2017G

نظام للكشف عن الغش في الامتحانات الإلكترونية

رزان حمزه باوارث

بحث مقدم لنيل درجة الماجستير في العلوم تخصص علوم حاسبات

د. عبدالله باسهيل
د. أنس فتوح
ا. د. شهاب جمال دين

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز
جدة – المملكة العربية السعودية

شعبان 1438هـ - مايو 2017م

Student Cheating Detection System in E-exams

By

Razan Hamza Bawarith

This thesis has been approved and accepted in partial fulfillment of the requirements for the degree of Master of Computer Science

EXAMINATION COMMITTEE

	Name	Rank	Field	Signature
Internal Examiner	Dr. Mohamed Yehia Dahab	Associate Professor	Computer Science	
External Examiner	Dr. Mohammad Hamza Awedh	Assistant Professor	Computer Engineering	
Advisor	Dr. Abdullah Ahmad Basuhail	Associate Professor	Computer Engineering	

KING ABDULAZIZ UNIVERSITY
Shaaban 1438H – May 2017G

Dedication

This work is dedicated to Mom and Dad, it's impossible to thank you adequately for everything you've done…

May Allah reward you.

Acknowledgment

At the outset all the thanks and praise is to Allah, by his generosity I finished this thesis. Also, it is with much appreciation and gratitude that I thank the following individuals who dedicated themselves to the successful completion of this thesis.

I would like to thank my supervisors Dr. Abdullah Basuhail, Dr. Anas Fattouh and Prof. Dr. Shehab Gamalel-Din. They gave me guidance throughout my research. Without his guidance, patience, and support this thesis wouldn't have been possible. The experience I gained from him will definitely influence the rest of my life.

I also owe many thanks to my brothers Mohammed, Saeed and Saleh and to my sisters Rawan and Renad.

Thank you to all my friends and my colleagues.

Many thanks go to the Deanship of Information Technology in KAU for their cooperation.

Razan Bawarith,

Apr 2017

Student Cheating Detection System in E-exams

Razan Hamza Bawarith

ABSTRACT

With the expansion of Internet and technology over the past decade, E-learning has grown exponentially day by day. Cheating in exams has been a widespread phenomenon all over the world regardless of the levels of the technology development. Therefore, detection of traditional cheating methods may no longer be wholly successful to fully prevent cheating during examinations. Online examination is an integral and vital component of E-learning. Students' exams in E-learning are remotely submitted without any monitoring from physical proctors. As a result of being able to easily cheat during e-exams, E-learning universities depend on an examination process in that students take a face-to-face examination in a physical place allocated on the university campus under supervised conditions, however this conflicts with the concept of E-learning. This thesis investigates the methods used by student for cheating in distance exams (D-exam) through: continuous authentication which refers to a method to guarantee that the authenticated person is the one who only takes the exam all over the entire exam session; and using online proctors which refer to effective methods to detect cheating in D-exam. In this thesis, we build an E-exam management system, which can detect the cheating in D-exam. The work of this system can be divided into two phases .The first phase is before being permitted to attend the D-exam session, Fingerprint Reader used to authenticate the examinee. The second phase is during the exam session, it is required to continuously guarantee that the examinee is the one who is claiming to be. Eye Tribe Tracker is utilized during the D-exam session. As result that; we can define the examinee status whether cheating or non-cheating exam through these two parameters: the total an examinee time on out screen and the number of times the examinee is out of screen. The approach that is proposed in this thesis is a novel technique applied in the E-exam management systems.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND TERMINOLOGIES

Symbol	Definition
D-Exam	Distance exam
E-Exam	Online exam
EMBA	Eye Movement Based Authentication
FPGA	Fingerprint Algorithm using A Spartan-6
HCI	Human-Computer Interaction
ICT	Information and Communication Technologies
IR	Infrared
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
RPNOW	Remote Proctor Now
SECONE	Security Control system in the Online Exam
SEE	Secure Exam Environment
TRA	Theory of Reasoned Action

Chapter one

Introduction

Chapter one

Introduction

1.1 Introduction

In recent years, information and communication technologies (ICT) witnessed rapid developments and had direct impacts on human life, especially in the field of education. ICT in education has a multiplier effect throughout the education system, by enhancing learning and providing students with new sets of skills; by reaching poor students or who have difficulty to reach educational institutions especially those in rural and remote regions. Interactive educational software combined with cheaper and more intuitive technology is used to ease interaction between teachers and students and raise the quality of knowledge by making it more accessible. As a result, E-learning has become increasingly popular over the last few years and widely adopted by universities and educational institutions. It enables to deliver information whenever students need anytime and anywhere through the web. For this reason, it is also called web-based learning or online learning.

“Assessment for Learning is the process of seeking and interpreting evidence for use by learners and their teachers to decide where the learners are in their learning, where they need to go and how best to get there” [1].

The Assessment is one of the main parts of the educational tasks. It takes an important place during the development of any e-learning course. Assessment is defined as a set of activities that includes testing, problem solving, development of collaborative or individual projects, participation in discussions, etc. These activities could be aggregated in an assessment unit. Assessment activities are used in measuring learning data collected about students learning achievement and evaluation in order to verify the acquired knowledge in the learning process, at the same time, to reflect the teaching effectiveness of instructors [2, 3].

Distance exam or D-exam is most widely used to assess student learning. Also, it is an efficient manner to conduct an examination. D-exams are a way of delivering questions to students who are not physically present in a traditional setting such as a classroom. They are created on basis of random questions per student with a specific time limit through which they are to be answered. Furthermore, they save or reduce time required for manual paper correction, as well as, it saves paper printing, thus protecting environment.

D-exam presents new challenges for teachers; notably, how to prevent students from cheating. Cheating on exams has been a widespread phenomenon in the world regardless of the levels of development. Different cheating patterns exist, such as copying the answer from the textbook, searching the internet for answers, discussing over email or message chat, and unauthorized person performing the exam instead of the authenticated one.

As a result, e-learning universities depend on an examination process in which students take a face-to-face examination in a physical place allocated over the university campus under supervised conditions to ensure the student identity. However, that conflicts with the concept of E-learning, which eliminates the temporal and spatial dimensions between the students and the learning process. Each student must be physically present in the classroom in order to take the exam.

This thesis investigated all types of method used for cheating in D-exam, and resolves this problem by either detection or prevention. Detecting and preventing cheating require a human intervention (i.e. the presence of a proctor). The proctor should authenticate students' IDs before starting the exam. However, this check is not enough. Continuous authentication all over the exam session is very necessary. In addition, we need a continuous process of monitoring and controlling over all students while taking the exam. Then, we also aim to investigate how to solve the cheating problem in D-exam through prevention and detection.

The continuous authentication is one of the methods that which designed to protect personal identity [15]. It attempts to verify that the users are during the examination, and will control if the current user is the same. Unlike face-to-face examinations, D-exam has no proctors or invigilators. They are held in a different and an uncontrolled remote environment. As a result, authentication goals in D-exam are important to check the identity of online students since it plays a key role in security [13, 14].

Fingerprints and eye tracking can be used to continuous authenticate the examinee. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprint identification is one of the most well-known and publicized biometrics, because of their uniqueness and consistency over time.

Fingerprint recognition has two stages: enrollment, in which, the user's fingerprint characteristics are measured and stored in the database; and verification, in which, the user's fingerprint characteristic is measured and compared with the database template.

Eye tracking is the process of measuring either the point of gaze to where one person is looking or the motion of an eye relative to the head. The eye gaze coordinates are calculated with respect to a screen the person is looking at, and are represented by a pair of (x, y) coordinates given on the screen coordinate system[45].

Online proctor (E-proctor) is another technique, which is planned to be investigated for the objective of monitoring a student while he/she is performing a D-exam. The E-proctor's role is to detect any cheating activities during the D-exam session.

E-exam management system is an application that is implemented in this thesis using the visual C# and SQL server database to detect and prevent the cheating in D-exam. E-exam management system used a Fingerprint Reader to authenticate the examinee, and Eye Tribe Tracker to continuously guarantee that the examinee is the one who is claiming to be. As a result, we can classify the examinee status as cheating or non-cheating according of two parameters: the total time the examinee is on out screen and the number of times the examinee is out of screen.

1.2 Motivations

E-learning becomes popular day by day as people are getting more and more concerned to add feather to their qualification. Online examination system is an efficient manner to conduct an examination. Examinee can appear from their convenient place and there is no need for traveling a distance. Online examination system also saves or reduces time

required for paper checking as well as it saves paper thus saving environment. We have more benefits on online examinations but cheating remains a problem.

The proposed of E-exam management system in this thesis tries to investigates all types of method used for cheating in D-exam.

1.3 Research Problem and Question

Cheating on exams has been a widespread phenomenon in the world regardless of the levels of development. Many studies have been conducted over the past decade about cheating activities performed by students and the means by which university could attempt to combat this problem [6]. The cheating problem in D-exam still not solves. Detecting and preventing cheating require a human intervention (i.e. the presence of a proctor). This proctor needs to physical authenticate students' ids before starting the exam. However, this is not enough; we need continuous authentication all over the exam session. In addition, we need a continuous process of monitoring and controlling over all students while taking the exam. Then, we also aim to investigate how to solve the cheating problem in D-exam through prevention and detection.

1.4 Goals

The main goal of this thesis is to implement and design a system that is capable of controlling the cheating in D-exam through either:

- ✓ Continuous authentication, which refers to a method to guarantee that the authenticated person is the one who only takes the exam all over the entire exam session.

- ✓ Using online proctors, which refer to effective methods to detect and prevent cheating in D-exam.

1.5 Methods

In order to satisfy these goals, we have investigated all types of methods used for cheating in D-exam. Detecting and preventing cheating require continuous authentication and online proctor. Before being permitted to attend a D-exam session, username/password, and fingerprints are used to authenticate the examinee. During the exam session, it is required to continuously guarantee that the examinee is the one who is claiming to be. Eye tracking is utilized during the D-exam session. The online proctor a technique that observing student via camera when he/she is taking a D-exam.

1.6 Thesis Outline

This thesis is organized into six main chapters described as follows:

Chapter 1 is an introduction which describes the research motivation, the problem Definition, and the approach of this research in attacking the problem.

Chapter 2 discusses existing works related to this thesis.

Chapter 3 presents necessary background about cheating on exams: the cheating concept, type of cheating, continuous authentication and E-proctor which are preventing cheating process.

Chapter 4 explains the E-exam management model implementation.

Chapter 5 fully detailed evaluation experiments are presented.

Chapter 6 draws the conclusion and discusses foreseen future work.

Chapter Two

Literature Review

Chapter Two

Literature Review

This chapter presents existing research studies that are conducted in order to solve the problem methods used by student for cheating in D-exam and continuously authenticating the student all over the exam.

2.1 Cheating

Students use many cheating techniques when taking examinations. Faucher and Caves [4] demonstrated the occurrence of cheating via giving, receiving and taking information and by circumventing in exam. Also, they presented some methods to detect and prevent cheating; moreover, academic integrity of the educational program needs to be maintained by using all resources available to develop effective policies and procedures.

Keresztury and Cser [5] evaluated cheating methods in classic exams which they classified into three categories: information exchange among students, using forbidden materials, and circumventing the process of assessment. However, new kinds of cheating appeared such as using information stored on a storage unit.

Methods of cheating have become ever more developed and hard to detect. Curran, Middleton and Doherty [6] highlight traditional methods cheating such as: hiding notes,

pencil case, writing on arms/hands and leaving the room. However, holding large amounts of information can be replaced by new technologies, for example using Mobile Phones, Calculators, MP3 Players, wireless receivers and Personal Digital Assistant (PDAs). In addition, they present technically feasible solutions that prevent the cheating process using signal jamming devices to identify mobile phones that are active and block communication among them.

Gao [7] summed the commonly used methods to prevent students taking online exams from e-cheating as follows; setting up time limitation; setting up quizzes and exams consisting of a set of randomly selected questions from a huge question pool so each student will have a different exam/test; comparing the IP addresses to see if two students are in the vicinity of each other; using biometrics to reduce the possibility of E-cheating and in order to authenticate remote students. Commonly biometrics includes keystroke, voice, signature, face, iris and fingerprint. In addition, he showed two commercially available products, which can be used to guarantee secure exams: Webassessor and ProctorU; that also has been tested via some universities and can be used to proctor e-exams.

Cheating in exam that a perpetual issue in advanced education; it's important to educators, researchers and the overall population alike. Williams, Abdullah and Owolabi [8] investigated of the relationships of gender, course of study, academic performance and position with cheating tendencies through students a Federal university in Nigeria. They looked into that 76.5% of the students seem cheating conduct; there was no course in which less than 66% of the students was contributory in cheating; a larger number of

males than females were contributory in cheating and low achievers cheated more than high achievers.

To perform online exams on student expands the likelihood for cheating by means of cut ,copy and paste of information to/from the testing environment , Screen capture and printing functions, Searching and surfing the Web, HTML source code seeing, send messaging, screen sharing. Frankl, Schartner and Zebedi [9] gave "Secure Exam Environment" (SEE) implemented at the Alpen-Adria-Universität Klagenfurt (AAUK) to be held on student portable pcs without access to local files and resource, for example, the Internet.

The web and the “anytime, anywhere“get to give by PDAs, put almost endless information at our fingertips. Numerous students have discovered clever approaches to utilize innovation to cheat during exams. Kelley and Dooley [10] highlight some of the most spread high tech cheating techniques such as smart phones. Text messaging answers back and forth with other test takers. Taking photos of the test with a phone and sending it to the second party for either copying or helping the first student. Storing data on graphics calculators can also be easily accomplished and recovered amid exams without the instructor realizing the student is cheating. Small mall micro-cameras and very tiny hearing aids allow a second party to view the exam, gaze the answer upward in a reference book and afterward transfer the answer to the exam taker.

As of late, it turned into the spread of college cheating then reasons why students cheat. Simkin and mcleod [11] talked about this issue in more depth. They applied the hypothesis the Theory of Reasoned Action (TRA) could expound cheating behavior, and identified what factors motivate students to cheat. Three factors of cheating motivators:

access to online resources; desire to succeed, and there is not existent punishments when a few instructors force for infractions. They displayed some of illustrations that using in cheating process. Text messaging to send test answers amid examinations, utilizing PDAs to take pictures and email test materials to others. They find that cheating is much more regular among business understudies than among non-business understudies.

Raines, Ricci, Brown, Eggenberger, Hindle, and Mara Schiff [12] focused on the students' definition of cheating in the online learning environment. However, they collected and analyzed for evidence of common words that give meaning to the definition of cheating. First, 60% of the students defined the cheating by breaking the principles, dishonesty and not using your own brain. Breaking the principles of the exam (expressed or implied),To get the answers by deceiving the teacher , storing answers on the memory of a calculator , and submitting answers that are not of your own creation ,for example.. Secondly, 39% of the students referred of cheating via focusing on the tangible outcomes of cheating, such that getting information by non-ethical means to pass an exam, and taking advantage of information or resources, known only by the cheater, to improve their grade. Finally, 3% of students were not able or willing to define cheating.

Cheating is clearly wrong, arguments against it, which it provides an unfair advantage, and obstructs learning. Obviously, the wrongness of cheating should be an ethical not a bureaucratic question. Bouville [13] discussed on the relationship between cheating and grades: cheaters get undeservedly high grades and thus an unfair advantage over other students. This may mean that the grade is an infallible evaluation of how good a student is, so that if grades are low it can only be because the student does not work enough.

Likewise, grades are a proxy for what students know and can do, which is in turn used as a proxy for what students may be able to do in the future.

2.2 Authentication

Authentication is one of the methods that were designed to protect personal identity [18]; also, attempts to verify that the users are who they claim to be. Unlike face-to-face examinations, D-exam has no proctors or invigilators. They are held in a different and an uncontrolled remote environment. As a result, authentication goals in D-exam are important to check the identity of online students since it plays a key role in security [16, 17].

There are two kinds of authentication [18]: static authentication and continuous authentication. Static authentication refers to authentication that takes places at the beginning of accessing the examination, and will be also valid during the whole examination until the user logs off from that examination. The continuous authentication refers to authentication that will be continued after the start of the examination, and will control if the current user is the same as the user who performs the initial exam.

Sabbah, Saroit, and Kotb [14] present a new method for e-examination authentication. This method enables educational institutions to manage cheating-free e-examinations, which has been considered a vital challenge for E-learning in the past decade. Also, they provide virtual, interactive, and secure E-examination sessions. They system requires user authentication that checks a user's identity whilst trying to access the system resources, and a proctor interactively and remotely monitors the examinees throughout their examination using a webcam and video call.

Jung and Yeom [15] suggested a Security Control system in the Online Exam (SECONE) that is based on group cryptography with an e-monitoring scheme. The cryptography supports enhanced security control for the online exam process, as well as authentication and integrity. However, it espoused two groups for secure communication between distributed entities in the online exam system. The intergroup communication protected via public key infrastructure (PKI) whilst the intragroup communication uses several symmetric Diffie-Hellman keys.

Most existing computer and network systems authenticate a user only at the initial login session. This could be a critical security weakness. Niinuma, Park and Jain [19] suggested a new framework for continuous user authentication that primarily uses soft biometric traits (e.g., color of user's clothing and facial skin). Soft biometric traits are defined as "those characteristics that give some data about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two people". Utilization of soft biometrics in a continuous authentication system has the following advantages: 1) user can be authenticated continuously even when either no hard biometric information or incomplete hard biometric data are available and 2) no preregistration of the soft biometric traits is required; the soft biometric traits are automatically enrolled every time the user logs in. They showed that the system is able to successfully authenticate the user continuously with high tolerance to the user's posture.

E-learning establishments are right now confronting two key difficulties identified with identity management. The customary static confirmation at login time whether it taking into account a straightforward secret key plan or a solid watchword is lacking. An understudy can undoubtedly impart their secret word to a specialist, and have that master take an online exam for their sake without being gotten, which is a genuine danger to the

respectability of the degrees offered by e-learning foundations. To prevent students from e-cheating continuous authentication are utilized. Continuous authentication is a guard constantly watching over who is utilizing a computer, utilizing facial features and soft biometric identifying attribute.

Continuous identity authentication can prevent an unauthorized individual from slipping in and utilizing the computer system after the initial authentication of the identity of the authorized user. Bhandwalkar and .Hanwate [20] displayed a new e-learning model used for identification, authentication and tracking the student. The system is robust with respect to user's posture in front of the workstation. Soft biometrics for continuous authentication offers high usability and, utilizing both soft and hard biometrics such as face recognition for relogin authentication, leads to higher security. Moreover, no additional hardware required for soft biometric.

The mainstream authentication techniques include fingerprint and eye track.

2.2.1 Fingerprint

Continuous Authentication is primary in online examinations where the user has to be continuously verified during the entire session. Sudarvizhi and Sumathi [21] tried to provide a comprehensive survey of research on continuous biometric authentication systems. Each biometric has its own strengths and weaknesses, and the choice depends on the application. It focused on Sclera and Fingerprint as their Multimodal biometric traits for continuous authentication of the user.

Online examinations are defined as E-examinations. They are taken over the Internet by a remote user. However, most systems used username/password method to identify the users. Wei, Cong and Zhiwei [22] proposed a fingerprint-based technology to identity

authentication rather than the traditional methods. A fingerprint identify/classify application and a load balance service are implemented on the examination server cooperated with the online examination system to accomplish authentication. The interfaces between the examination system and the identity authentication application can use code embed methods or SDK invoking methods to adapt different fingerprint sensors. The identity authentication works well in the Internet/intranet online examination systems.

Biometric technology includes the identification and verification of individuals via analyzing the human body characteristics. It has been widely utilized in various aspect of life for different purposes, in particular as regards this study the issue of staff attendance. Oloyede, Adedoyin and Adewole [23] conducted a study using a telecommunication company in the South West region of Nigeria, to decide the particular biometric identifier that can used to enhance their traditional staff attendance system. They demonstrate that fingerprint is the best biometric technology system that can sustainably solve the lingering problem of staff attendance in the proposed organization.

Fingerprint authentication is one of the most reliable and widely utilized personal identification methods. Shinde and Bendre [24] design and implementation of an Embedded Fingerprint Authentication system that works in two phases: minutia extraction and minutia matching. Also, they explained the hardware-software co-design responsible for matching two fingerprint minutiae sets and suggests the use of reconfigurable architectures for Automatic Fingerprint Authentication System. In addition, they implemented a Fingerprint Algorithm using A Spartan-6 (FPGA). The experimental results demonstrate that system meets the response time requirements of

Automatic Fingerprint Authentication System with high speed utilizing hardware-software co-design.

Fingerprint verification is an important biometric technique for personal identification. Jain, Lin Hong, Pankanti and Bolle [25] implemented a prototype automatic identity-authentication system that uses fingerprints to authenticate the identity of an individual. They enhanced minutiae-extraction algorithm, which is capable of finding the correspondences between input minutiae and the stored template without resorting to exhaustive search and has the ability to compensate adaptively for the nonlinear deformations and inexact transformations between an input and a template. The experimental results uncover that system can accomplish a good performance on these data bases ;additionally , it can a complete authentication procedure on average takes about 1.4 seconds on a Sun ULTRA 1 workstation .

2.2.2 Eye Tracker

Eye tracking technology is an assistant channel to Human-Computer Interaction (HCI). Applications of eye movements to real time user interfaces can be separated into two classifications: (1) using eye movements as an straightforwardly control tool, for example, a non-touchable mouse pointer for the disabled , and (2) analyzing eye movements to get the user's intention and then to facilitate the interaction environment, for example, interactive graphical displays and interface usability measurements . The application of eye tracking technology in authentication offers a promising and feasible solution to the tradeoff between the ease of use and the security of an authentication system. Zhang, Zheru and Dagan [26] decomposed the Eye Movement Based Authentication (EMBA) technique into three basic aspects: (1) eye movement input

modality, (2) eye movement interaction mechanism, and (3) eye movement pattern recognition. They researched EMBA system is still in its early stages. A large portion of the reported cases are only prototypes without providing substantial system error analysis and extensive usability test.

A real-time authentication system means that it opens up the possibility for greater security; however such a system must be unobtrusive and secure. Recent advances in the capabilities of commercial remote eye tracking devices and decreases in their cost may lead to their utilization for user-friendly, secure, continuous biometric authentication. Mock, Hoanca, Weaver, and Milton [27] studied whether a commercial eye tracker can be utilized for user authentication via iris recognition. They used a k-nearest neighbors algorithm and just the right iris, the same information ,set allowed 100% accuracy for k = 3 . They research iris recognition by an eye tracker might enable real-time continuous authentication when combined with other more reliable authentication such as password.

The improvement of eye tracking systems represented a challenge for researchers and different organizations in the range of IT. Lupu and Ungureanu [28] reviewed eye tracking technique that is depends on a device to track the movement of the eyes to know exactly where the person is looking and for how long. It also includes software algorithms for pupil detection, image processing, data filtering and recording eye movement by means of fixation point, fixation duration and saccade as well. They displayed some application of eye tracking, for example, human computer interaction, brain computer interaction, assistive technology, e-learning, psychology investigation, and pilot training assistance, virtual and augmented reality.

Eye tracking is becoming a well-known technique with regards to the usability research. With the help of an eye tracker the user’s pupils and their position on a screen are

followed and thus provide detailed data about the user's visual attention on user interface elements. It can be utilized as a valuable source of information about user's behavior. Manhartsberger and Zellhofer[29] investigated eye tracking is a valuable instrument to improve the findings of qualitative usability testing .also; the eye tracking data is importance of interpreting within the context of the user interface.

Numerous eye-tracking systems either require the user to keep their head still or involve cameras or other equipment mounted on the user's head; however. These constraints make the systems unacceptable for prolonged use in interactive applications. Meyer, Böhme, Martinetz, and Barth [30] used eye trackers for improved visual communication through gaze guidance. The eye tracking systems that utilize single-camera remote eye tracking system, it accomplishes accuracy in the range of 0.5 to 1.0 degrees. However, No accuracy measurements have been made yet on the complete system, but tests on simulated data show the gaze estimation algorithm can achieve an accuracy of one degree or better.

Eye tracking systems have numerous potential applications, for example, learning emotion monitoring systems, drivers' fatigue detection systems, etc. Su, Wang and Chen [31] used an eye tracking system to implement an "eye mouse" to give computer access for individuals with severe disabilities. The eye mouse permits people with severe disabilities to utilize their eye movements to manipulate computers. It requires only one low-cost Web camera and a personal computer. They developed a five phase algorithm to evaluate the directions of eye movements and then use the direction information to manipulate the computer. Experiments were show that it can be used to manipulate the computer for individuals with severe disabilities.

2.3 Proctors

E-learning is a commonly accepted model for learning with a large number of suppliers utilizing platforms to deploy materials and educate students. Whilst many efforts have been spent on the creation and deployment of Virtual Learning Environments, less focus has been given to the related problem of providing e-invigilation. Clarke, Dowland, and Furnell [32] have presented an approach to supply remotely based e-Invigilation of assessments through the use of transparent biometrics. This eliminates the need to have physical invigilators, allocated classrooms or assessment centers and it provides both the assessor and the candidate with a degree of freedom; yet providing the level of safety you would expect from a formal assessment procedure.

Online education has become a major force in advanced education. Both the number of students taking online courses and the number of courses offered are grown at a double digit rate. Faculty has been reluctant to adopt online courses without some assurance of honesty by the course participants. In response to this concern, new technologies are emerging to verify the identities of online course participants and to reduce the opportunities for academic dishonesty. Cluskey, Ehlen, and Raiborn [40] have introduced the Software Secure remote E-proctoring .This system needed to 360 degree camera that recording the test. The system could prove to be an asset to institutions seeking to expand or improve their online course offerings

2.3.1 ProctorU

ProctorU is a portion of a cottage industry of online proctoring suppliers that has grown in recent times as universities and colleges have set their sights on nontraditional students who need to get degrees without leaving home [33]. ProctorU is a proctoring

service, which allows students to take proctored exams via web camera. The main feature of using ProctorU is that it allows students to take exams under supervision without having to move to different testing center [34]. The student is linked to real persons who guide him/her through the process. They watch the test taker's screen in real time and can view everything the student is doing both at the location and on screen [35].

2.3.2 Tegrity

Tegrity's Remote Proctoring feature ensures the integrity of exams taken off campus. The student can take their exam at their home while Tegrity records video of the student taking the test, along with the associated screen activity. The recordings cannot be paused while the student takes the exam, and when completed, the recording is immediately uploaded for instructors [37].

2.3.3 B Virtual

B Virtual collaborates with higher education institutions to create custom, live, online exam proctoring services [37]. B Virtual's allows students to take their exams from the comfort of their homes in a live, proctored and secure environment. Furthermore, B Virtual can be record all exam session data including video, audio and keystroke information to monitor of student [38].

2.3.4 ProctorCam

ProctorCam is an online proctoring solution for test takers and administrators. Test takers schedule their test from website with a proctor. ProctorCam monitor test takers anywhere in the world using desktop, audio and webcam monitoring technologies [39].

2.3.5 Kryterion

The Kryterion Online Proctoring system is requires a proctor who supervises the administration of a test and a student's utilization of a webcam and microphone. Online proctoring enables test takers to schedule and take an online exam anytime, anywhere, while our certified proctors ensure adherence to your testing standards. The proctor monitors the session electronically for suspicious behavior or violations to testing standards [41].

2.3.6 ProctorCam Remote Proctor Now

Remote Proctor Now (RPNOW) is a self-service model for secure online examination delivery and identity verification. Utilizing a standard computer webcam with an internet connection that recording all sound and videos, a 360-degree view of the exam environment, students can take a proctored exam online conveniently and affordably. RPNOW is Flexible for students which provide freedom to take exams at times and dates convenient for them; no scheduling required [42].

2.3.7 ProctorFree

ProctorFree is an automated, exam proctoring solution that requires no human inclusion. ProctorFree authenticates the student utilizing facial recognition and maintains continuous identity verification throughout the exam via webcam. Additionally, it gives a secure browser that is fully customizable to allow student’s flexibility to access certain web pages or applications, provided that is allowed for that particular exam. Throughout the exam ProctorFree also monitors for a variety of events, behaviors, and patterns typically associated with cheating. The administrator can log into ProctorFree’s review dashboard to easily sort and view results. Also ,it highlight the specific minute and

second where cheating-like behaviors occurred and allow the administrator to determine if the student cheated or not[43].

2.3.8 ProctorExam

ProctorExam offers a web-based platform for Safe Online Exams. Also, identify the exam taker behind the computer and create a highly secure exam environment in order to deliver high-stakes exams. The student shares the screen with Proctor to ensure that they are just utilizing whitelisted programs and websites. Using web camera built into the computer to capture a full 360 degree view of the exam environment. The proctor will watch and make notes of any anomalous behavior of the student, and can immediately alert the institution to any behavior that falls outside proper test taking parameters [44].

Chapter Three

E-Exam Management Model

Chapter Three

E-Exam Management Model

In this chapter, we give an overview of exam, type of exam, cheating and cheaters' methods, continuous authentication via fingerprint and eye tracking, and online proctor.

3.1 Exam

Exams are most widely used to assess student learning. Furthermore, they help prevent students from information release in the course. Students want to process information in one-way or another in order to learn.

However, exams can be classified into three types: traditional exams, online exams and D-exam.

3.1.1 Traditional Exam

Traditional exam are defined as a set of questionnaires given in the class. They are created on static questions per student. As a result, all students must start and finish the exam at the same time.

3.1.2 Online Exam

Online exams, sometimes referred to as e-examination, are an Internet based exams. They are created on random questions per student with specific time limits through which they are to be completed. Furthermore, students should attend to a classroom for performing the exam.

3.1.3 Distance Exam

Distance exams (D-exams), are a way of delivering questions to students who are not physically present in a traditional setting such as a classroom. They are created on random questions per student with specific time limits through which they are to be answered. Further, D-exams allow students to perform the test at anytime and anywhere.

3.2 Cheating

Cheating is an act of falsehood, deception, swindle‹, quackery, or imposition employed to create an inequitable advantage often at the expense of others. Cheating implies the breaking of rules. A general zone for cheating is to be practiced during examinations.

Cheating on exams has been a widespread phenomenon in the world regardless of the levels of development. Many studies have been conducted over the past decade about cheating activities performed by students and the means by which university could attempt to combat this problem [6]. In the U.S., it was revealed that 80% of the higher achieving secondary school students admitted to cheat in during exams, 95% of secondary school students who admitted cheating said that they had not been caught, 51% of secondary school students did not believe cheating was wrong, 85% of college students said cheating was necessary to get ahead, 75% of college students admitted

cheating in exams, and 90% of college students did not believe cheaters would be caught [53].

The most common reasons that motivate students to cheat include: pressure from parents to do well, fear of failure, unclear instructional objectives, desire for a better grade, everyone else is doing it, there is no punishment if being caught, there is little chance of being caught, no time to study, and easy access to online information [54].

It is easier to fight against cheaters if one understands their methodology. There have been studies researching cheaters' methods, which can be classified into three levels: traditional cheating, online cheating in class and distance cheating.

3.2.1 Traditional Cheating

Many students still use traditional cheating methods that are defined as each student can be cheating by one or others. As a result, it can be classified into two types: individual cheating and group cheating. Individual cheating refers to when a student cheats by oneself via writing on his/her body parts, or on a small note and hiding it in clothes. Group cheating refers to the case when students share information with others using hand gestures especially fingers to communicate with others, giving the recipient student clues to the correct answers.

3.2.2 Online Cheating

Traditional cheating that appears in online exam is called online cheating. Student can be cheating via the Internet. However, it can be classified to two types: individual cheating and electronic cheating. Individual cheating refers to when a student tries to cheat by self by writing small notes and hiding them in clothes, using the calculator, iPod or mobile, for example. Electronic cheating refers to when students share

information with others via Internet, for example, sending a question to an expert via email or chat.

Table 1 explains the different types of cheating in both traditional and online exams. In addition, it presents some of the suggested solutions to prevent and detect cheating; by proctor we mean a person who monitors or invigilates exams.

Table 3.1 Types of Cheating in Exams

	Type	Traditional Cheating		Online Cheating	
		Prevention	**Detection**	**Prevention**	**Detection**
1	Looking at another student's paper/answer sheet or work. This is preplanned by student's colluding to sit in such a way to coordinate copying [53]	Leave empty area between students or create different samples of the exams	Seek help from physical proctors		
2	Communicating with sign language or a code for transmitting answers such as clicking of pencils, foot tapping, and cap turning on head or body gestures. [53]	Create different samples of the exams	Seek help from physical proctors		
3	Writing on desks: especially when written in pencil for easy wiping later [56]	Check all desks before starting the exam	Seek help from physical proctors		
4	Using cheating sheets: prewritten cheat sheets, usually in small font, hidden in clothes or under wrist watch [56]		Seek help from physical proctors		Seek help from physical proctors
5	Using cheating sheet on the floor: prewritten cheating sheets hidden in books or under folders below the desk [56]	Make sure that books or notes are stored in backpack, not under	Seek help from physical proctors	Make sure that books or notes are stored in backpack, not under	Seek help from physical proctors

		desk		desk	
6	Faculty giving opportunity to students to go to the bathroom, allowing students to review notes hidden in the trashcan in the bathroom [57].		Do not allow examinees to go the bathroom Or on breaks		Do not allow examinees to go the bathroom Or on breaks
7	Using numeric devices to communicate a question number or correct answer by text messaging via cell phones [57]	Don't allow cell phones or use a Microsoft Dongle to detect any Devices with Bluetooth technology in the "on" Position	Seek help from physical proctors	Don't allow cell phones or use a Microsoft Dongle to detect any Devices with Bluetooth technology in the "on" Position	Seek help from physical proctors
8	Copying test questions and sending them to someone by email or chat [57]			Using software that don't allow examinees to run any application	Seek help from physical proctors
9	Using any sort of text-based memory calculators to record all the equations, notes, theorems, proofs, etc. [56]	Use simple calculators	Seek help from physical proctors	Use simple calculators	Seek help from physical proctors
10	Listening to the iPod which has recording abilities; It is possible to hide earphone wires behind long hair [56]	Don't allow examinees to use iPod's	Seek help from physical proctors	Don't allow examinees to use iPod's	Seek help from physical proctors

3.2.3 Distance Cheating

D-exam is an efficacious manner to conduct an examination. Students can study from any convenient place. Moreover, there is no need for physical traveling. However, it faces the problem of cheating during examinations since there are not physical proctors invigilating and controlling the exam. This is referred to as distance cheating. Distance cheating includes all previous kinds cheating.

In addition to that, there are other forms of cheating, such as:

- Taking an examination for another student.
- Using programs that help to solve the exam questions.
- Copying exam question and sending them to an expert to send back the answers.
- Downloading resources from the Internet, for example, using an e-book.
- Looking up answers via the Internet.
- Using cell phones, and the internet to search for an answer of question.
- Using a cell phone camera to take pictures of the exam.
- Using chat rooms on the web to get solution of exam.

3.3 Continuous Authentication

3.3.1 Fingerprint

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprint identification is one of the most well-known and publicized biometrics, because of their uniqueness and consistency over time .No two people has exactly the same fingerprints. Even identical twins, with identical DNA, have different fingerprints. This uniqueness allows fingerprints to be used in all sorts of ways, including for background checks [45].

Fingerprint offer many advantages:

- ✓ Uniqueness - Fingerprints of each finger of our ten fingers are distinctive, different from one another and from those of other persons. Even identical twins have different fingerprints.
- ✓ Convenience - Users no longer have to remember multiple, long and complex, frequently changing passwords or carry multiple keys.
- ✓ Non-repudiation - Ensures the user is present at the point and time of recognition and later cannot deny having accessed the system.
- ✓ Non-transferable - Cannot be shared, lost, stolen, copied, distributed or forgotten unlike passwords, PINs, and smart cards.
- ✓ Proven - Long history of successful use in identification tasks - the U.S. and other countries have extensive real-world experience with fingerprint recognition. Fingerprints have been used in forensics for well over a century and there is a substantial body of scientific studies and real world data supporting the distinctiveness and permanence of fingerprints.

3.3.1.1 Fingerprint Characteristics

Fingerprint ridges are not continuous straight ridges. Instead, they are broken, forked, interrupted or changed directionally. The points at which ridges end, fork, and change are called minutiae points which provide distinctive, identifying information. The most common properties of fingerprint minutiae points are [46]:

- ✓ Type: There are several types of minutiae points: crossover, core, bifurcations, ridge ending, island, delta and pore; as is shown in Figure 3.1.
- ✓ Direction

- ✓ Position

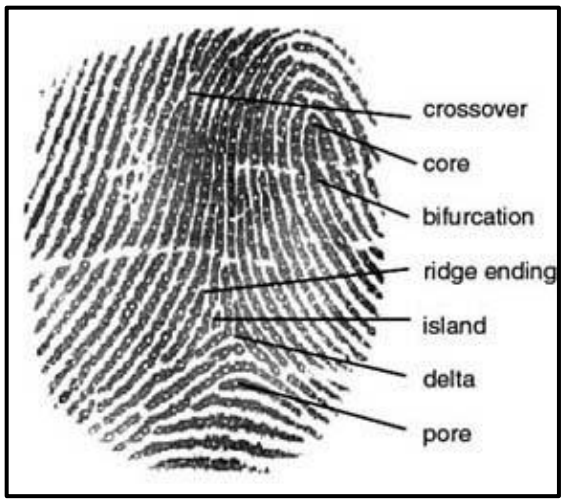

Figure 3.1 Fingerprint Minutiae Properties [46]

3.3.1.2 Fingerprint Recognition

Fingerprint recognition operates in two distinct modules: enrollment and verification, as is shown in Figure 3.2. [47]:

1. Enrollment Module: an application for users to enroll. It performs the following functions :
   - ✓ Captures multiple fingerprints for at least two fingers using a fingerprint reader.
   - ✓ Checks image quality to ensure that a good quality scan is obtained.
   - ✓ Extracts the fingerprint minutiae.
   - ✓ Saves the fingerprint images and/or minutiae in a database.
2. Verification Module: an application that verifies users. It performs the following functions:
   - ✓ Captures a fingerprint from a fingerprint reader.
   - ✓ Extracts the fingerprint minutiae.

- ✓ Compares fingerprint with enrolled fingerprints to identify a user from a list or verify a specific user.

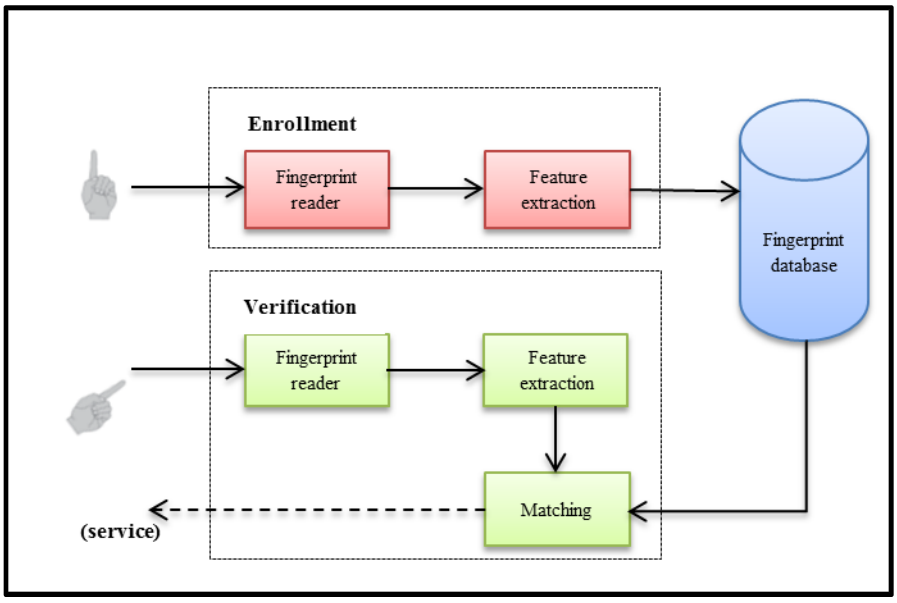

Figure 3.2 Fingerprint Recognition Systems [47]

3.3.2 Eye Tracking

Eye tracking is the process of measuring either the point of gaze where one is looking or the motion of an eye relative to the head. An eye tracker is a technique for detecting the position where the eye is looking.

Eye tracking is a technology that finds out the eye gaze point of a user as he or she looks around. The eye gaze coordinates are calculated with respect to a screen the person is looking at, and are represented by a pair of (x, y) coordinates given on the screen coordinate system[48].

Eye tracking can be used in a wide variety of applications typically categorized as active or passive. Active applications involve device control, for example aiming in games, eye activated login or hands-free typing. Passive applications include performance analysis

of design, layout and advertising. Other examples are vehicle safety, medical diagnostics and academic research [52].

3.3.2.1 Eye Tracking Features

- ✓ Eye Position: When the eye is presented with a stimulus, the eye follows a specific pattern unique to an individual.
- ✓ Eye Velocity: The underlining principle used in eye-position can be extended to the time-domain by taking the change of eye position with respect to the time leading to the eye velocity.
- ✓ Eye Movement Direction: The direction in which the eye moves is unique
- ✓ Signal: The eye velocity coupled with the eye movement gives it a high potential feature.
- ✓ Eye Distance: The position of eye in the horizontal and the vertical directions [49].

3.3.2.2 Methods of Eye Tracking

A method of recording eye position and movements is called oculography. There are three different methods to track the motion of the eyes [51]:

- ➢ Electro-Oculography

In this method, sensors are attached at the skin around the eyes to measure an electric field exists when eyes rotate. By recording small differences in the skin potential around the eye, the position of the eye can be estimated, as is shown in Figure 3.3.

Figure 3.3 Electro-Oculography of Eye Tracking [51]

- Infrared Oculography

The infrared (IR) oculography measures intensity of reflected infrared light. In this eye tracking method, eye is illuminated by infrared light which is reflected by the sclera. The difference between the amounts of IR light reflected back from the eye surface carries the information about the eye position changes. The light source and sensors can be placed on spherical glasses.

- Video Oculography

A video-based eye tracker is to estimate the direction of gaze from the picture delivered by a video camera. A possible way is to detect the iris using the high contrast of the white of the scelra and the dark iris. The most video-based eye trackers work with the detection of the pupil. There are two methods to detect the pupil – the dark and the bright pupil method. With the dark pupil method an image processing technique locates the position of a black pupil in the camera image. The bright pupil method uses infrared light reflected from the retina and this makes the pupil to appear white in the camera image [50].Video-based eye tracking is the most widely used method in commercial eye trackers. Video oculography make use of single or multiple cameras to determine the movement of eye using the information obtained from the images captured.

3.4 Online Proctor

Online proctor (E-proctor) is another technique, which is planned to be investigated for the objective of monitoring a student while he/she is taking a D-exam. The E-proctor role is to detect any cheating activities during the D-exam session.

In literature, as well as commercially, there are many trials for online proctor systems, such as: Software Secure, ProctorU, Tegrity, Respondus, ProctorCam, B Virtual, and Loyalist.

E-Proctor is an integrated solution that brings academic integrity to distance learning exams. The E-proctor requires fingerprint scanner to authenticate the identity of a student, and eye tracker contain a camera to track the user's eye movement. The camera tracks even the most minuscule of movements of the users' pupils, by taking the images and running them through computer-vision algorithms. The algorithms read "on-screen gaze coordinates" and help the software to then determine where on the screen the user is looking. E-proctor is connected to the student' computer, which locks the computer into the exam program while simultaneously prohibiting access to all applications or pre-existing information, which could be used to cheat during an exam.

The student must successfully pass through the ID authentication stage which entails placing their finger on a scanner which will match their biometrics with the one gathered during initial registration .Also , the student needs a personal calibration process due to the fact that each person has different eye characteristics, and the eye tracking need to estimate gaze accurately. The calibration consists of a circular target that is displayed at different locations of the screen on a blank background for around 2 seconds per each

location. The user needs to look at the target as it is displayed on the screen. Once all the calibration targets are displayed on the screen the calibration process is completed.

Once student identification process authenticated and calibrated, E-proctor launches the exam application while locking the computer system until the exam completed. During the exam, E-proctor will record changes in eye movement, as is shown in Figure 3.4. The approach that is proposed of e-proctor is a novel technique applied in the D-exam.

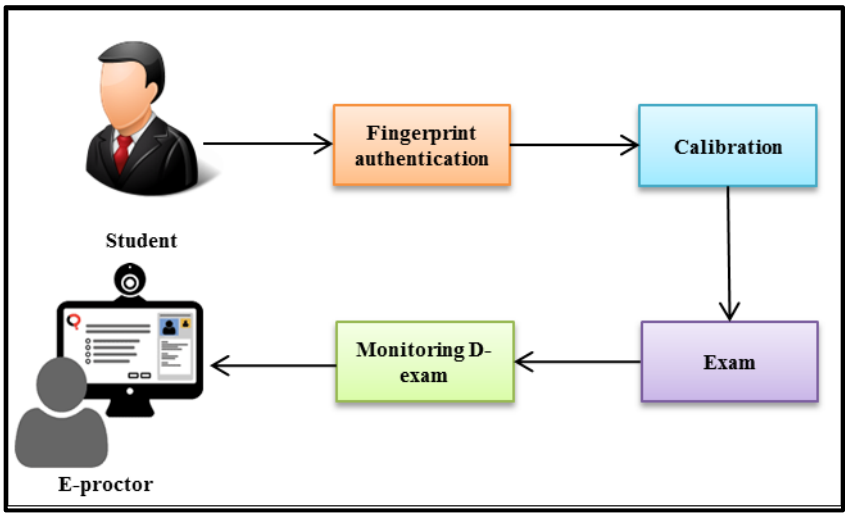

Figure 3.4 Online Proctor

Chapter Four

E-Exam Management Model Implementation

Chapter Four

E-Exam Management Model Implementation

In this chapter, we describe E-Exam Management System Architecture, and use case diagram model. Furthermore, we discuss in details the implementation of E-Exam Management System

4.1 E-Exam Management System Architecture

E-exam management system is an application that establishes a network between the E-learning institute and the students. Institute's instructors upload to the site the questions of the exam. These questions are displayed as a test to the eligible students. The answers entered by the students, then evaluated and their scores are calculated and saved. These scores can access by the institute to determine the passed students or to evaluate their performance.

The work of E-exam management system can divided into two phases; as depicted in Figure 4.1. The first phase is before being permitted to attend the E-exam session in this phase, username/password and fingerprints must be used to authenticate the examinee. The second phase is during the exam session; it is required to continuous guarantee that

the examinee is the one who is claiming to be. Eye tracking utilized during the E-exam session.

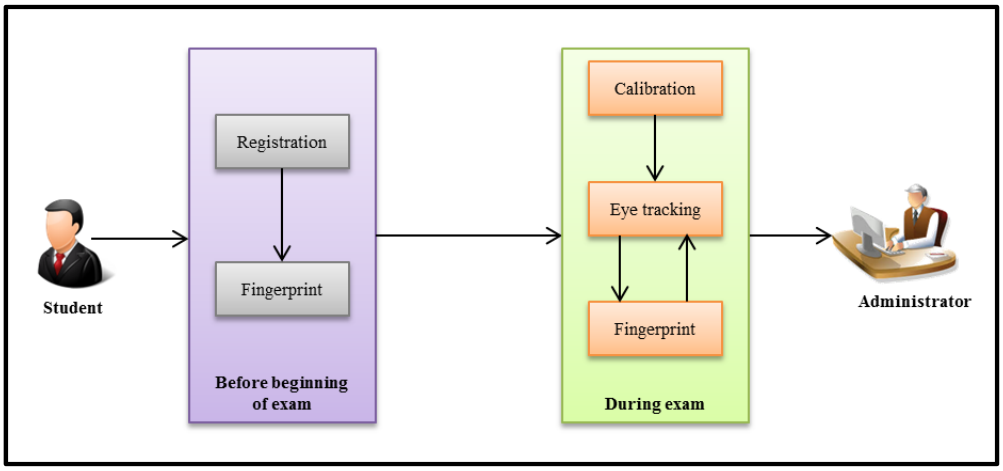

Figure 4.1 Architecture of E-Exam Management System

4.1.1 Before Starting Exam

- ✓ **Registration**

  The system user, i.e. the examinee, first must create an account. The user will be requested to provide his/her user name which will be used as the core identification to the system. The user will be requested to choose his/her password which will enable him/her to log into the system. After registration, the examinee is being able to enroll by the fingerprint to the system.

- ✓ **Enrollment by Fingerprint**

  When building an enrollment fingerprint in system, the data flow consists of:

1. Capture a Fingerprint Image (scan) from the fingerprint reader. The resulting Fingerprint Image Data (FID) contains one or more fingerprint images, called a Fingerprint Image Views (FIVs).
2. Extract the fingerprint features. During extraction, Fingerprint Minutiae Data (FMD) is created, with each fingerprint stored in a Fingerprint Minutiae View (FMV) in the FMD. FMDs used for identifying users in a collection and verifying specific users.

4.1.2 During Exam

In this phase, the examinee may continuously authenticate through an eye tracking to prevent any cheating activity. Eye tracking is the process of using sensors to locate features of the eyes and estimate where someone is looking (point of gaze).The tracker must be placed below the screen and pointing at the examinee. The examinee needs to be located within the tracker's trackbox. A trackbox is a small graphical component that illustrates an examinee's position relative to the sensor, as shown in Figure 4.2. This is useful to see if the person is within the range of the sensor and that tracking is fully functional. After that, the examinee will now be ready for the calibration process.

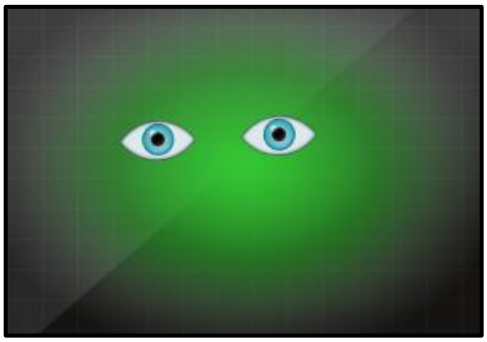

Figure 4.2 Trackbox

✓ **Calibration Process**

The calibration process requires examinee to look at a series of calibration targets distributed evenly throughout the screen. Each target will appear one-by-one and they are visible for a predefined time period. The process usually takes about 20 seconds to complete, as shown in Figure 4.3.

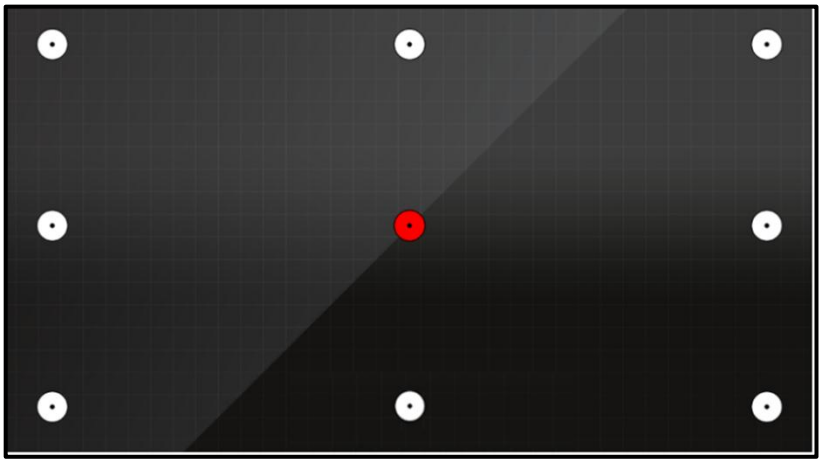

Figure 4.3 Calibration Process

✓ **Eye Tracking**

After calibrate process is successful, the examinee will now be able to log into E-exam. The examinee may continuously authenticate through an eye tracker. Eye trackers may be able to prevent any cheating status on E-exam. Eye tracking data collected using either a remote or head-mounted 'eye tracker' connected to the computer. Each eye data observation is translated into a set of pixel coordinates so that the presence or absence of eye data points in different screen areas can be examined. This type of analysis is used to determine which features are looked at, when a particular feature captures attention, how quickly the eye moves, what content is overlooked and virtually any other gaze-related question.

To achieve the continuous authentication in E-Exam Management system via eye tracker, the system needs to distinguish between three scenarios as shown in Figure 4.4.

Scenario 1:

The examinee is in front of the screen and his frontal eyes view is available to the camera.

Scenario 2:

The examinee is sitting in front of the screen, but he is looking either left, right, up, or down.

Scenario 3:

The examinee has moved away from the screen.

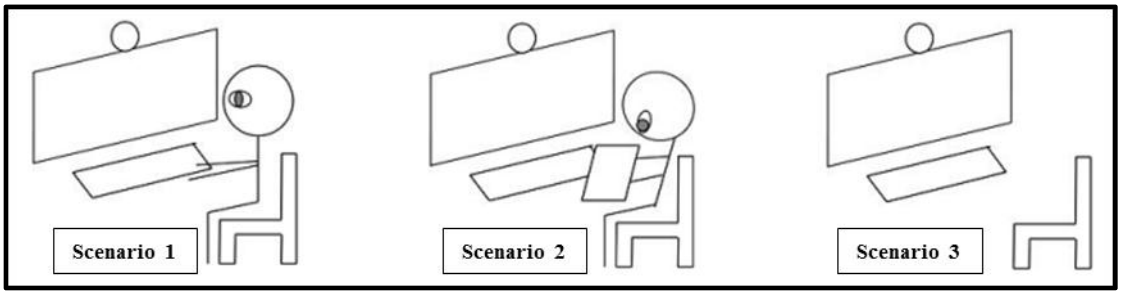

Figure 4.4 Scenarios of Eye Tracking

In scenario 1, the system is un looked the exam, because examinee is active and in front of the screen, also the system can be monitoring the examinee via eye tracker .In scenario 2 and scenario 3, the system locked the exam after five minutes; because the user is not active or moves away from the screen, furthermore the system must re-authenticate examinee automatically.

4.2 E-Exam Management System Algorithm

E-exam management system that we suggested in this thesis consisted of several modules that perform the functions of the system. Figure 4.5 demonstrates flowchart of the algorithm of the E-exam management system.

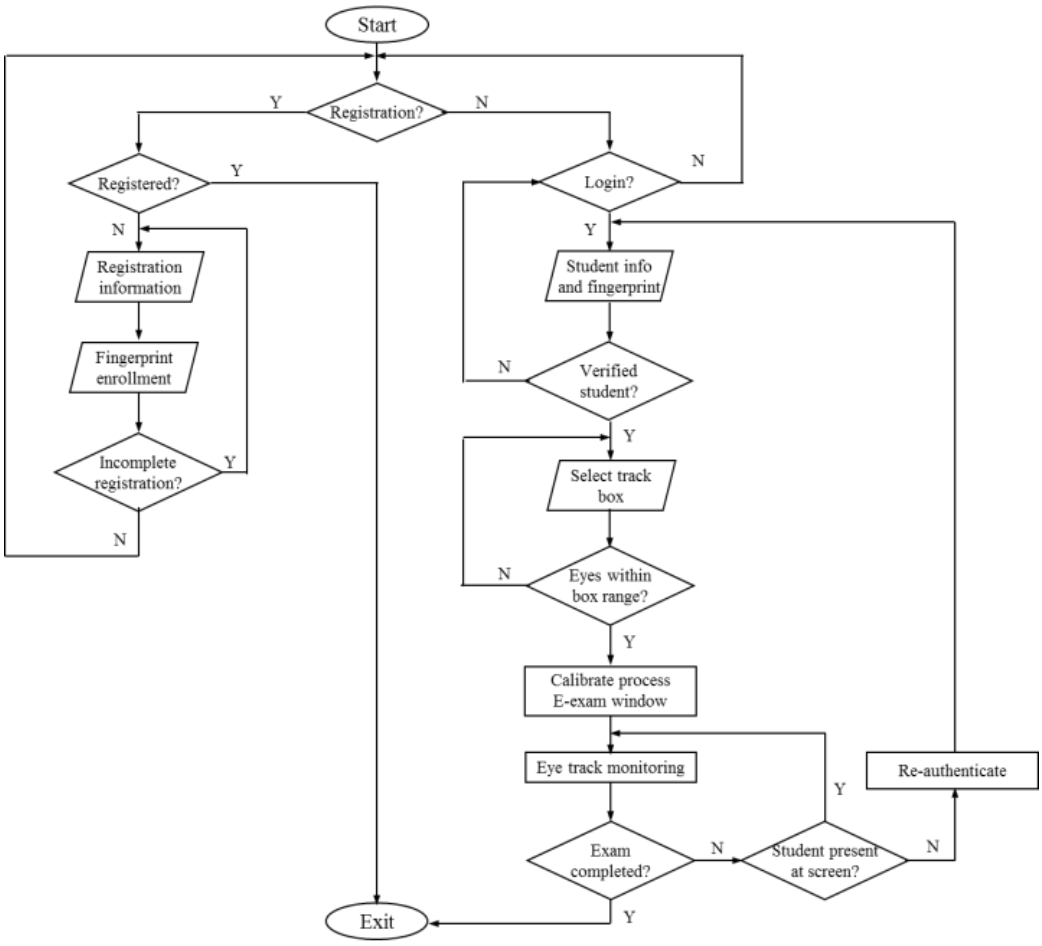

Figure 4.5 Flowchart of E-Exam Management System

4.3 Use Case Diagram of E-Exam Management Module

Use case diagram are usually referred to as behavior diagram used to describe a set of actions (use case) that E-exam management system can perform in collaboration with

two actors (admin and user). Each use case should provide some observable and valuable result to the actors or other stakeholders of the system, as shown Figure 4.6.

1. User registration by administration when using the system the first time.
2. Authenticate user when login the system or during E-exam.
3. Now the user can log into E-exam after complete authentication process and calibration process.

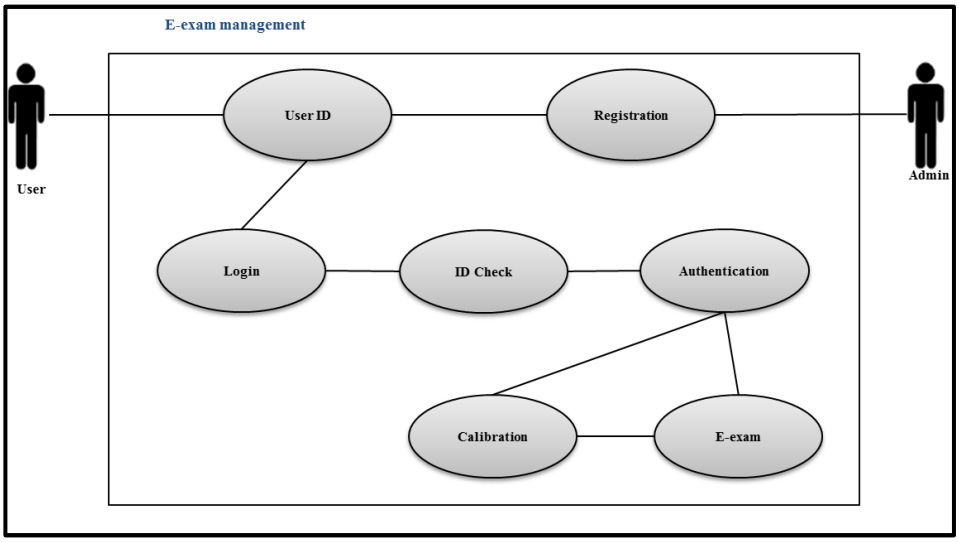

Figure 4.6 Use Case of E-Exam Management System

4.4 The Implementation of E-Exam Management System

4.4.1 Programming Language and Tool

E-Exam Management system is implemented using visual C# 2012 programming language and SQL server 2008 database. We build the system as an application.

In our system, we need some hardware as follows:

- ✓ Digitalpersona U.are.U 4500 HD USB Fingerprint Reader

The U.are.U 4500 Reader utilizes optical fingerprint scanning technology to achieve excellent image quality, a large capture area and superior reliability, as shown in Figure 4.7. We use this tool for continuous authentication process.

Figure 4.7 Digitalpersona U.are.U 4500 HD USB Fingerprint Reader

- ✓ Eye Tribe Tracker

The Eye Tribe Tracker utilizes a camera and a high-resolution infrared LED to track the user's eye movement, as shown in Figure 4.8. We use this tool for online proctor.

Figure 4.8 Eye Tribe Tracker

4.4.2 E-Exam Management System Interface

The following snapshots of the program demonstrate E-Exam Management systems.

First window (Figure 4.9) of our proposed system that contains the following buttons: register and login.

Figure 4.9 Main Windows

Second window (Figure 4.10) is registering the student via administrator. The admin can fill the information of student such as ID, First name, Last name and password.

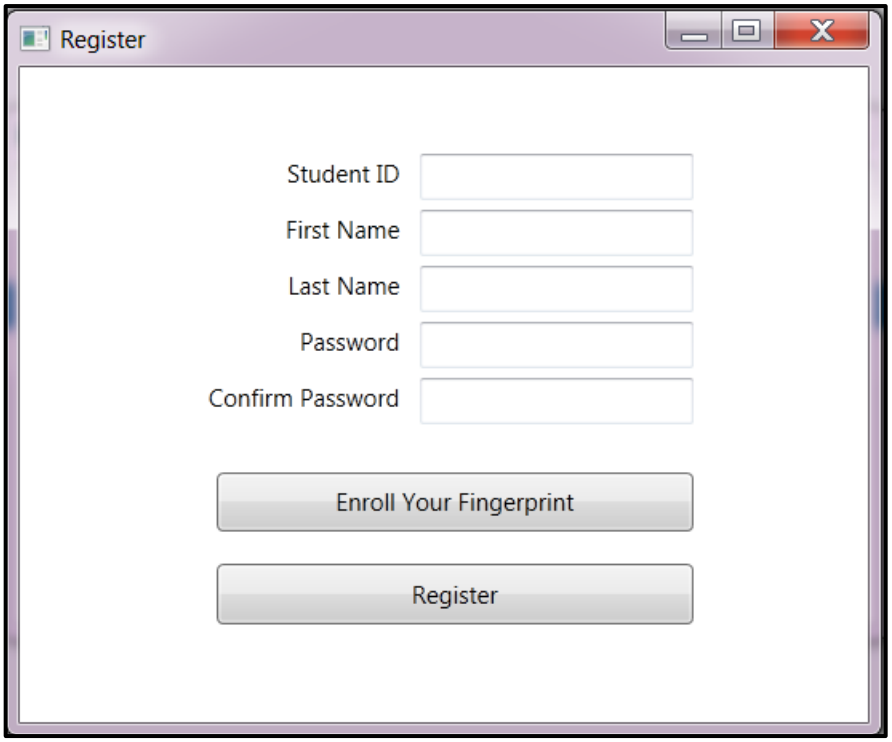

Figure 4.10 Student Registration

A third window (Figure 4.11) is student fingerprint enrollment via U.are.U 4500 HD USB Fingerprint Reader.

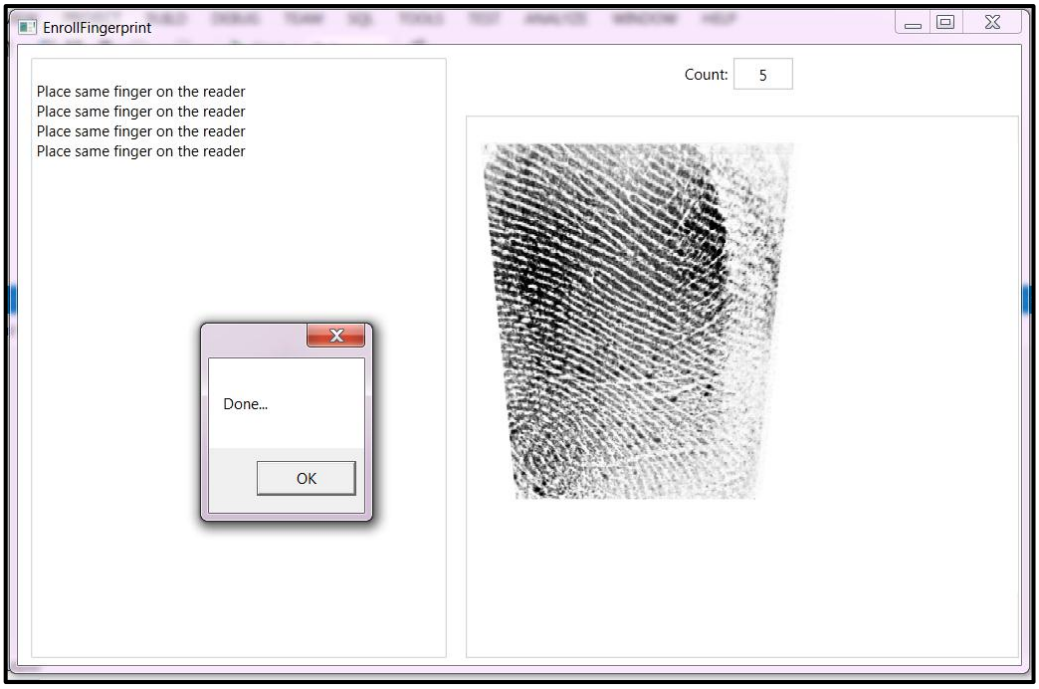

Figure 4.11 Enroll Fingerprint

Fourth windows (Figure 4.12) is the login of the student into the exam, the user can enter the ID, password, and enroll fingerprint.

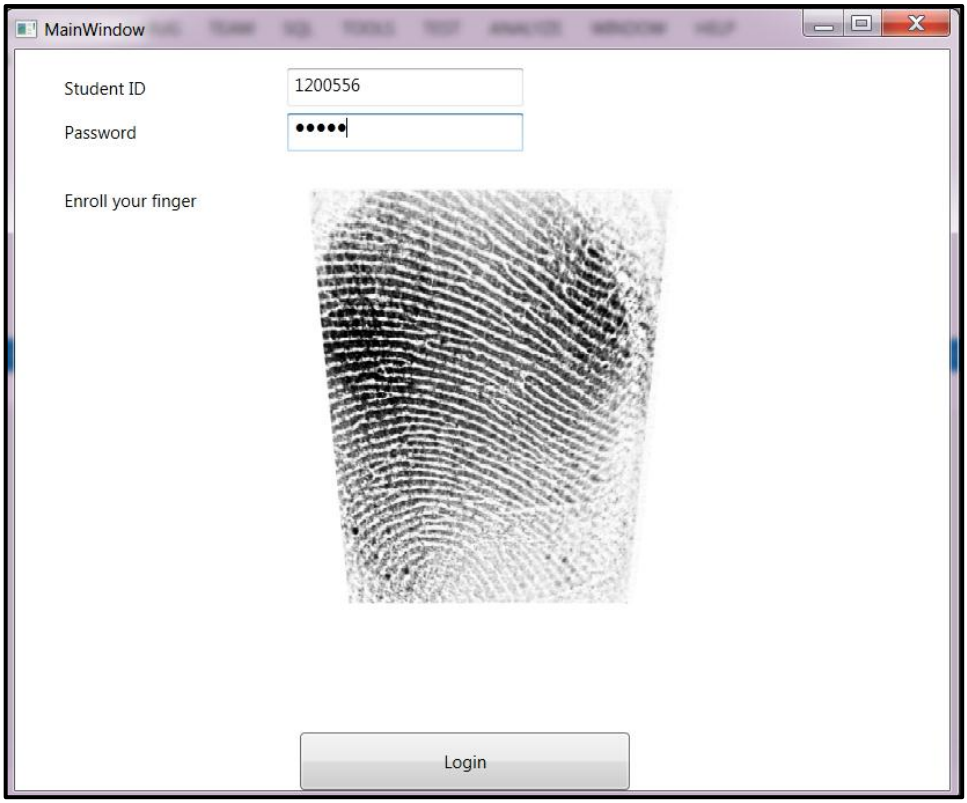

Figure 4.12 Login into Exam

Fifth window (Figure 4.13) is selection trackbox by Eye Tribe Tracker, which is useful to see if you are within range of the sensor and tracking.

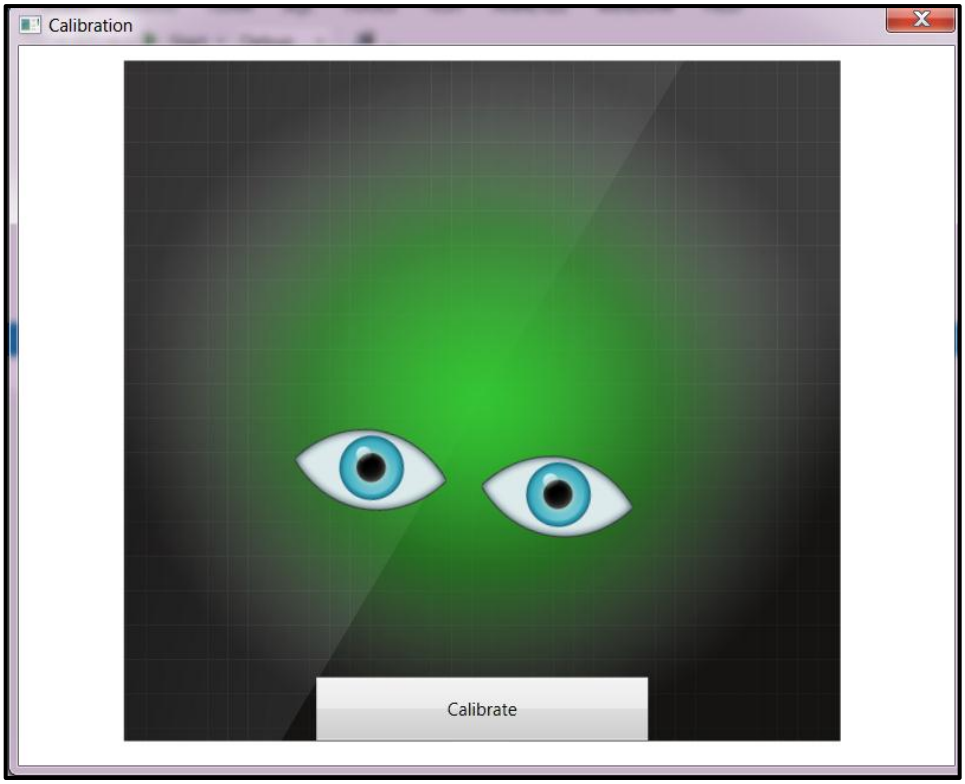

Figure 4.13 Selection Trackbox

Sixth window (Figure 4.14) is the calibration process, which used for estimation of eye position.

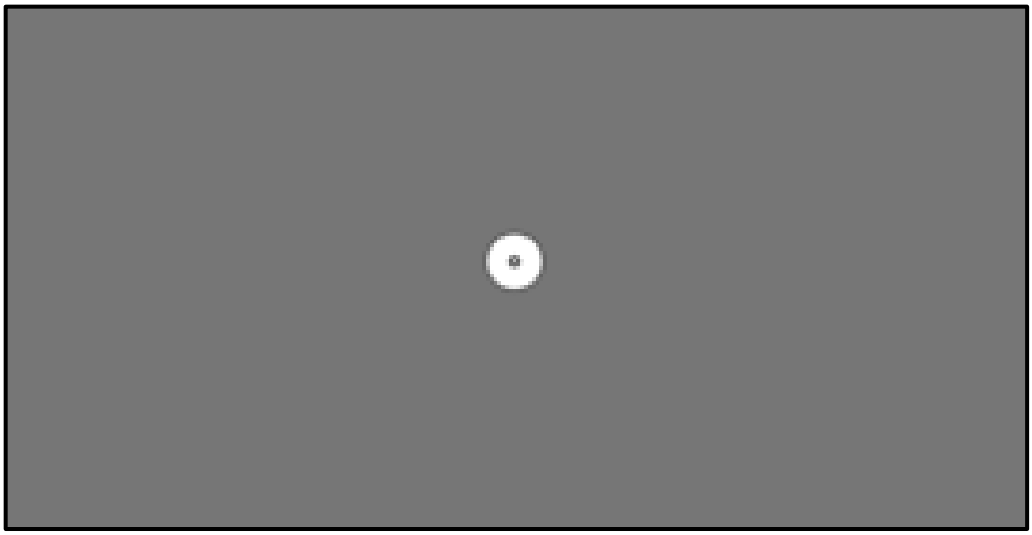

Figure 4.14 Calibration Process

Seventh window (Figure 4.15) is an E-exam window that monitoring eye tracker. Any time, E-Exam System recognizes that the examinee is no longer present in front of the screen. The system is locked and it must re-authenticate the examinee automatically via fingerprint, as shown in Figure 4.16.

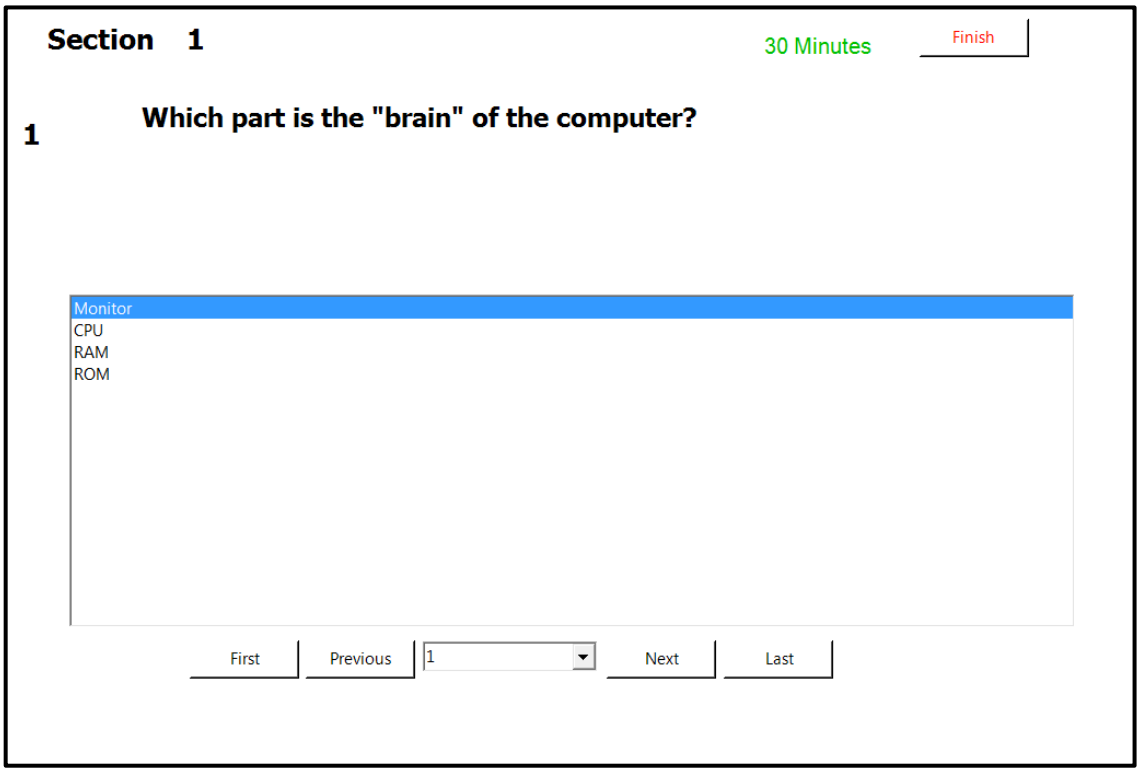

Figure 4.15 E-Exam Windows

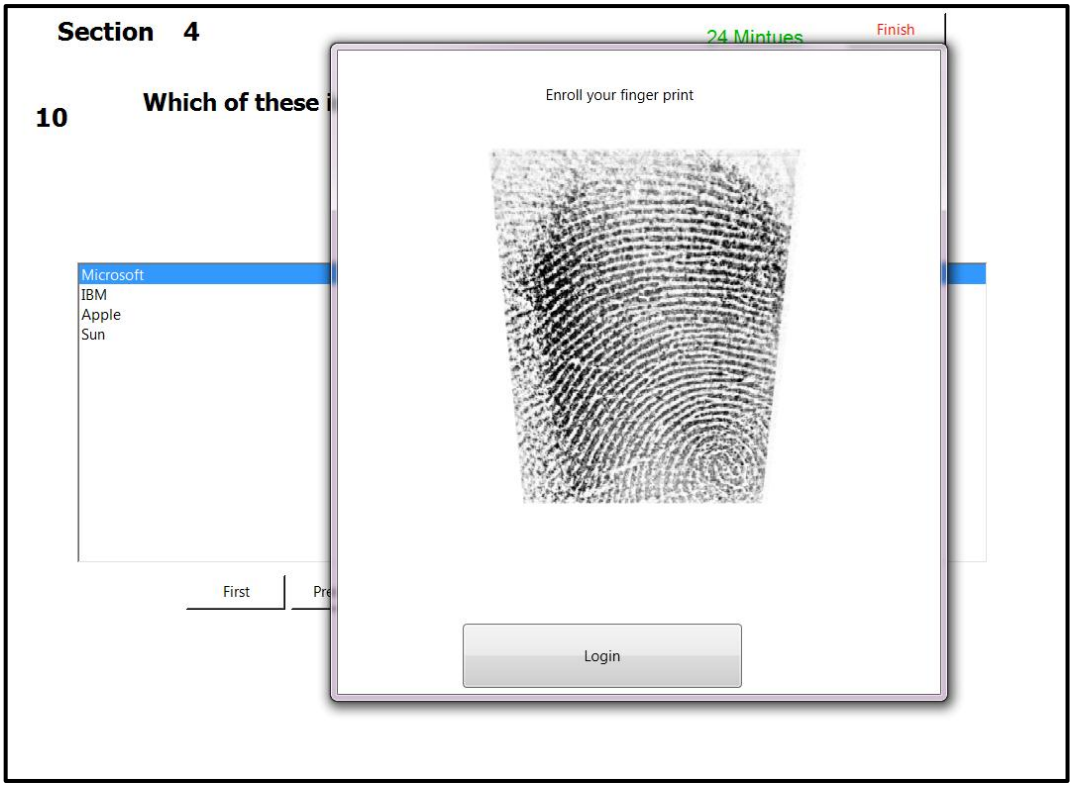

Figure 4.16 Re-Authenticate Users via Fingerprint

Chapter Five

Analysis and Evaluation

Chapter Five

Analysis and Evaluation

In this chapter, we demonstrate how we collect our data. After that, we discuss evaluation of the results obtained by our proposed system.

5.1 Experiment Design

The E-exam management utilized to detect any status of cheating in D-exam. In this experiment, we used the fingerprint reader for continuous authentication examinee and eye tribe tracker for observation of examinee through D-exam.

5.2 Data Collection

The experiments involved 30 participants. Participants were divided into two groups: the first group consisted of 15 participants who were in status of cheating during the D-exam, and the second group was 15 participants who were in status of non-cheating during the D-exam. In addition, each participant repeated the experiment three times. In this situation, the size of data equals 90 samples in this experiment.

We observed the participant in D-exam via the eye tracker. The tracker registers the movements of the participant's eyes in a database. The database contains the user ID of

the examinee, the time when the student gets out of the screen, the time when the student comes back to the screen, and the cheating status. Tables 5.1 show samples of collected data.

Table 5.1 Samples of Collected Data

Sample #	The time out of the screen (Second)	The number of times out of the screen	Status
1	98	10	non- cheating
2	388	28	non- cheating
3	149	16	non- cheating
4	91	12	non- cheating
5	863	32	cheating
6	738	21	cheating
7	1015	11	cheating
8	906	21	cheating

5.3 Data Analysis

A scatter plot of the data is shown in Figure 5.1.

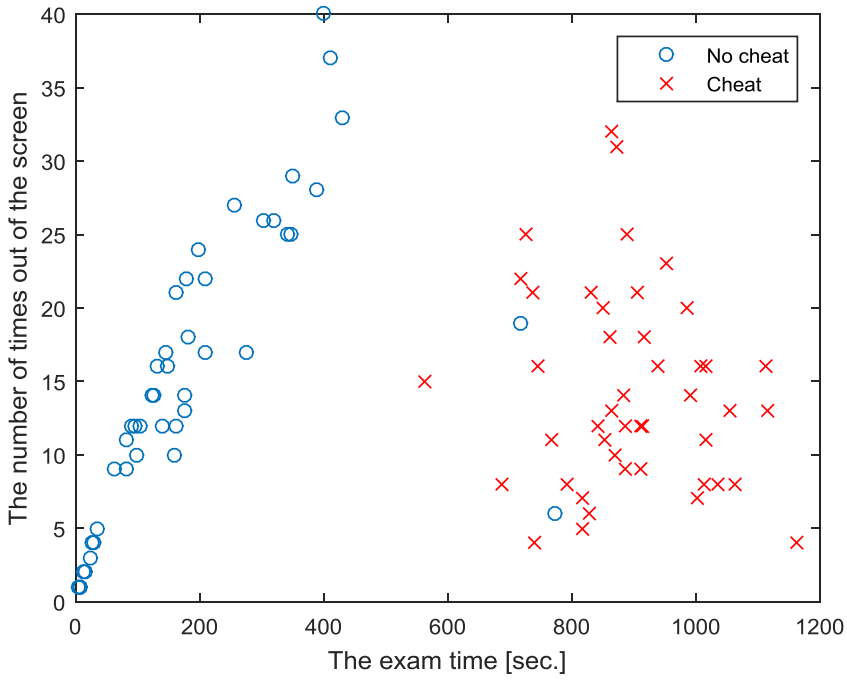

Figure 5.1 Scatter Plots of 90 Samples

We can discriminate between “cheating” case and “no cheating” case by dividing the plane into two regions by a line defined by the two points p1 (300, 0) and p2 (600, 40) as shown in the following Figure 5.2.

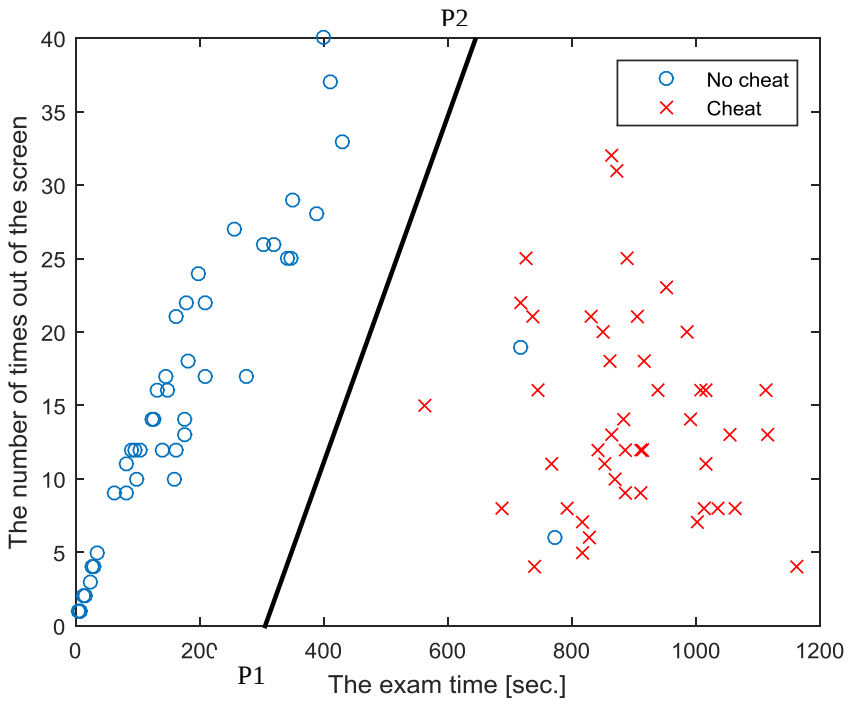

Figure 5.2 Scatter Plots of 90 Samples with a Separation Line

Let t be the exam time when the student get out of the screen and n be the number of times out of the screen, then the equation of the line is:

$$n = m\,t + b \tag{1}$$

Where m is the slope of the line and b is the intercept. They can be calculated as follows.

$$m = \frac{\Delta n}{\Delta t} = \frac{40-0}{600-300} = \frac{2}{15} \tag{2}$$

$$b = n - m\,t = 0 - \frac{2}{15} \times 300 = -40 \tag{3}$$

Therefore, the equation of the line is:

$$n = \frac{2}{15}\,t - 40 \tag{4}$$

Any sample $s(t_s, n_s)$ can be classified using equation (4) as follows:

$$s \in \begin{cases} no\ cheating & if\ n_s - \frac{2}{15} t_s + 40 > 0 \\ cheating & if\ n_s - \frac{2}{15} t_s + 40 < 0 \end{cases} \quad (5)$$

Using the classifier defined by the equation (5), the 90 samples can be classified as shown in Figure 5.3.

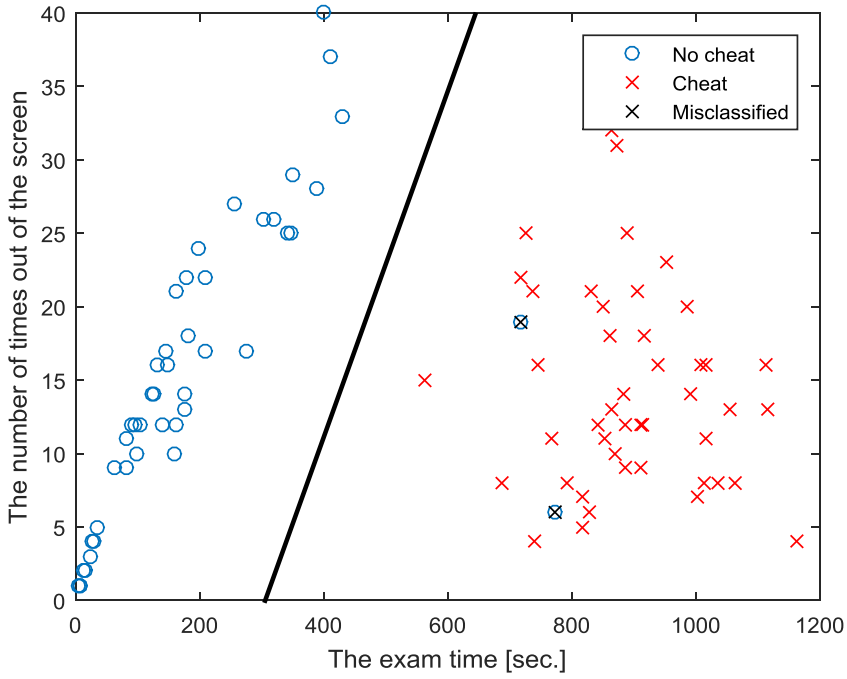

Figure 5.3 Classifying the 90 Samples Using Equation (5)

5.4 Discussion of Results

In this type of experiment, we use the most commonly used methods for measuring correctness and quality of the information-retrieving application: sensitivity, specificity, precision, accuracy, and F-measure. These measurement approaches clarify the precise percentage of the classifier's effectiveness and accuracy [58].

A confusion matrix, also known as a contingency table used to indicate the results of the recall, specificity, precision, and accuracy measures. The confusion matrix contains four cells:

- ✓ TP: Number of true items on the classified positive samples.
- ✓ FP: Number of false items on the classified positive samples.
- ✓ TN: Number of true items on the classified negative samples.
- ✓ FN: Number of false items on the classified negative samples.

The confusion matrix is given by:

Table 5.2 Confusion Matrix

	Predicted No	**Predicted Yes**
Actual No	43	2
Actual Yes	0	45

Therefore,$TN = 43$,$FP = 2$, $FN = 0$, and$TP = 45$. In addition; the performance of the Table 5.2 is measured as follows:

- ✓ Sensitivity (Recall) which is measures the proportion of positives that correctly identified, also called the true positive rate.

  Sensitivity (Recall) = TP / (TP + FN) = 100 %
- ✓ Specificity, which is, measures the proportion of negatives that correctly identified also called the true negative rate.

  Specificity = TN / (FP + TN) = 95.56 %
- ✓ Precision is the fraction of retrieved instances that are relevant, also called positive predictive value.

Precision = TP / (TP+FP) = 95.74%

- ✓ Accuracy is the proximity of measurement results to the true value.

  Accuracy = (TP + TN) / (TP + TN + FP + FN) = 97.78 %

- ✓ F-measure: A measure that merges both the precision and the recall, also called the harmonic mean.

  F-measure = 2*TP / (2*TP+FN+FP) = 97.83%

Chapter Six

Conclusion and Future Work

Chapter Six

Conclusion and Future Work

This chapter concludes the work conducted throughout this thesis. Section 6.1, reviews the thesis results and highlights the main contributions. Moreover, section 6.2, demonstrates the limitation, and section 6.3, points out few future research directions.

6.1 Conclusion

This thesis addresses the issues surrounding the student cheating in online exam. It introduces the basic concepts of cheating a how it can be used in online exam. It provides some of methods that detecting and preventing student's cheating trough online exam. Continuous authentication is one of the methods that attempts to verify that the users are present during the examination, and will control if the current user is the same. Furthermore, online proctor is another technique that is to detect any cheating activities during the D-exam session.

E-exam management system is proposed to investigate cheating in D-exam using Fingerprint Reader to authenticate the examinee, and Eye Tribe Tracker to continuous guarantee that the examinee is the one who is claiming to be. This system developed in visual C# and SQL server database to detect and prevent the cheating in D-exam. As a

result, we can classify the examinee status as cheating or non-cheating according of two parameters: the total time the examinee is on out screen and the number of times the examinee is out of screen. The approach that is proposed in this research is a novel technique applied in the E-exam management systems.

To evaluate this proposed work, a series of experimental test conducted. The test yielded the following results: sensitivity is 100 %, specificity is 95.56 %, precision is 95.74%, accuracy is 97.78 %, and F-measure is 97.83%.

6.2 Limitations

There are two limitations of the system that we presented in this thesis. The first limitation is the handling of the cases of students with special needs. Problems have occurred when the student's head is normally tilted or student has a significant problem with one eye. The second limitation is that the system can't work effectively with some students. Problems have occurred when some students, who wear eyeglasses or contact lenses, had small pupils, or have long eyelashes.

6.3 Future Work

There are several promising directions to extend the work presented in this research. The system can be implemented over the web. Another feature to improve continuous authentication is to use voiceprint that can be integrated and utilized during the D-exam session. Using face recognition as continuous authentication, which can identify a specific individual in a digital image by analyzing and comparing patterns. Still one more enhancement can be made is that, after a student start an exam, the use of keystrokes as continuous authentication that will control whether the current user is the

same as the user who initiated the static authentication or not. Furthermore; Add additional tests by using data that has not been tested on testing module via machine learning.

List of References

1. Assessment Reform Group, "Assessment for Learning: 10 Principles,"2002. [Online].Available: https://assessmentreformgroup.files.wordpress.com/2012/01/10principles_english.pdf&gt [Accessed: 23- Mar- 2017].

2. R. Barchino, J.M. Gutierrez, S. Otón, J.J. Martínez, J.R. Hilera and J.A. Gutierrez, "E-Learning Model for Assessment," PROCEEDINGS OF THE IADIS VIRTUAL MULTI CONFERENCE ON COMPUTER SCIENCE AND INFORMATION SYSTEMS (MCCSIS2006),pp.59-63, 2006.

3. U. Jamornmann and Techniques for Assessing Students, "E-Learning Achievement," International Journal of the Computer, vol.12 (2), pp.26 -31, 2004.

4. D. Faucher and S. Caves, "Academic dishonesty: Innovative cheating techniques and the detection and prevention of them," Teaching and Learning in Nursing, vol.4 (2), pp.37-41, 2009.

5. B. Keresztury and L. Cser, "New cheating methods in the electronic teaching era," Procedia-Social and Behavioral Sciences, vol.93, pp.1516-1520, 2013.

6. K. Curran, G. Middleton and C. Doherty, "Cheating in exams with technology," 2011.[Online].Available: https://pdfs.semanticscholar.org/1ba7/bc7b96f0bbc3ecbbcd958f9bd755852c1c02.pdf [Accessed: 23- Mar- 2017].

7. Q.Gao, "Online teaching: Do you know who is taking the final exam," 2012. [Online].Available: https://www.asee.org/documents/sections/middle-atlantic/fall-2010/01-Online-teaching-Do-you-know-who-is-taking-the-final-exam.pdf [Accessed: 23- Mar- 2017].

8. F.A. Olasehinde-Williams, I.O. Abdullah and H.O Owolabi, "The relationship between background variables and cheating tendencies among students of a federal university in Nigeria,"Nigerian Journal Educafional Foundafions, vol.6 (1), pp.68-79, 2003.

9. G. Frankl, P. Schartner and G. Zebedin, "Secure online exams using students' devices," Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), Marrakech, pp. 1-7, 2012.

10. R. Kelley and B. Dooley, "The technology of cheating," 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, Chicago, IL, pp. 1-4, 2014.

11. M.G. Simkin and A. McLeod, "Why do college students cheat?,"Journal of Business Ethics, vol. 94(3), pp.441-453, 2010.

12. D.A. Raines, P. Ricci, S.L. Brown, T. Eggenberger, T. Hindle and M. Schiff, "Cheating in Online Courses: The Student Definition," Journal of Effective Teaching, vol.11 (1), pp.80-89, 2011.

13. M. Bouville, "Why is cheating wrong?," Studies in Philosophy and Education, vol.29 (1), pp.67-76, 2010.

14. Y. Sabbah, I. Saroit and A. Kotb, "An interactive and secure e-examination unit (ISEEU)," 2011 RoEduNet International Conference 10th Edition: Networking in Education and Research, Iasi, pp. 1-5, 2011.

15. I. Y. Jung and H. Y. Yeom, "Enhanced Security for Online Exams Using Group Cryptography," in IEEE Transactions on Education, vol.52(3), pp. 340-349, Aug. 2009.

16. A. Ullah, H. Xiao and M. Lilley, "Profile based student authentication in online examination," International Conference on Information Society (i-Society 2012), London, pp. 109-113, 2012.

17. A. Ullah, H. Xiao and M. Lilley and T. Barker, "Using challenge questions for student authentication in online examination," International Journal for Infonomics (IJI), vol.5 (3/4), pp.9, 2012.

18. P. Bours and H. Barghouthi, "Continuous authentication using biometric keystroke dynamics," Norwegian Information Security Conference (NISK), November 2009.

19. K. Niinuma, U. Park and A. K. Jain, "Soft Biometric Traits for Continuous User Authentication," in IEEE Transactions on Information Forensics and Security, vol. 5(4), pp. 771-780, Dec. 2010.

20. K.T. Bhandwalkar and P.S. Hanwate, "Continuous User Authentication Using Soft Biometric Traits for E-Learning, "2014. [Online]. Available: http://www.ijirset.com/upload/2014/special/vishwatech/Paper-35_Continuous.pdf [Accessed: 23- Mar- 2017].

21. S. Sudarvizhi and S. Sumathi, "A review on continuous authentication using multimodal biometrics," Int J Emerg Technol Adv Eng, vol.3, pp.192-196, 2013.

22. L. Wei, Z. Cong and Y. Zhiwei, "Fingerprint Based Identity Authentication for Online Examination System," 2010 Second International Workshop on Education Technology and Computer Science, Wuhan, pp. 307-310, 2010.

23. O. Oloyede Muhtahir, O. Adedoyin Adeyinka and S. Adewole Kayode, "Fingerprint Biometric Authentication for Enhancing Staff Attendance System," vol.5 (3), 2013.

24. A. S. Shinde and V. Bendre, "An Embedded Fingerprint Authentication System," 2015 International Conference on Computing Communication Control and Automation, Pune, pp. 205-208, 2015.

25. A. K. Jain, Lin Hong, S. Pankanti and R. Bolle, "An identity-authentication system using fingerprints," in Proceedings of the IEEE, vol. 85(9), pp. 1365-1388, Sep 1997.

26. Y. Zhang, Z. Chi and D. Feng, "An Analysis of Eye Movement Based Authentication Systems, " In International Conference on Mechanical Engineering and Technology (ICMET-London 2011), ASME Press, 2011.

27. K. Mock, B. Hoanca, J. Weaver and M. Milton, "Real-time continuous iris recognition for authentication using an eye tracker, "In Proceedings of the 2012 ACM conference on Computer and communications security,pp.1007-1009, 2012.

28. R.G. Lupu and F. Ungureanu, "A survey of eye tracking methods and applications," Bul Inst Polit Iasi, pp.71-86, 2013.

29. M. Manhartsberger and N. Zellhofer, " Eye tracking in usability research: What users really see, " In Usability Symposium, vol.198 (2), pp. 141-152, 2005.

30. A. Meyer, M. Böhme, T. Martinetz and E. Barth, "A single-camera remote eye tracker, " In International Tutorial and Research Workshop on Perception and Interactive Technologies for Speech-Based Systems, pp. 208-211, 2006.

31. M.C. Su, K.C. Wang and G.D. Chen, "An eye tracking system and its application in aids for people with severe disabilities," Biomedical Engineering: Applications, Basis and Communications, vol.18 (06), pp.319-327, 2006.

32. N. L. Clarke, P. Dowland and S. M. Furnell, "e-Invigilator: A biometric-based supervision system for e-Assessments," International Conference on Information Society (i-Society 2013), Toronto, ON, pp. 238-242, 2013.

33. S. Kolowich, "Behind the Webcam's watchful eye," 2013. [Online].Available: http://www.chronicle.com/article/Behind-the-Webcams-Watchful/138505/ [Accessed: 23- Mar- 2017].

34. T. Community, "Proctored testing - Tallahassee community college," 2017. [Online].Available: http://www.tcc.fl.edu/student-life/student-services/testing-center/proctored-testing/ [Accessed: 23- Mar- 2017].

35. "Why not to use Proctoru.com," [Online]. Available: http://stop-proctoru.blogspot.com/ [Accessed: 23- Mar- 2017].

36. Tegrity, "Remote Proctoring," 2015. [Online]. Available: http://www.mhhe.com/tegrity/products/remotE-proctor ing.html [Accessed: 23- Mar- 2017].

37. B. Corporation, "B virtual," 2003. [Online]. Available: https://www.bomgar.com/resources/case-studies/b-virtual [Accessed: 23- Mar- 2017].

38. "Academic Honesty and Cheating on Online Course Exams,". [Online]. Available: http://facultyecommons.com/wp-content/uploads/2012/07/Academic-Honesty-Document-7.2012.pdf [Accessed: 23- Mar- 2017].

39. N. RENO, "The AIPMM partners with ProctorCam to strengthen academic integrity of online exams, "2012. [Online].Available http://www.prweb.com/releases/2012/7/prweb9710096.htm [Accessed: 23- Mar- 2017].

40. G.R. Cluskey Jr, C.R. Ehlen and M.H. Raiborn, "Thwarting online exam cheating without proctor supervision, "Journal of Academic and Business Ethics, vol.4, pp.1, 2011.

41. "Kryterion online proctoring," [Online].Available: https://www.onlineproctoring.com/home.html [Accessed: 23- Mar- 2017].

42. "Secure testing | online proctor, " 2017. [Online].Available: http://www.softwaresecure.com/ [Accessed: 23- Mar- 2017].

43. "Proctor Free| online Proctoring," 2013. [Online].Available: http://proctorfree.com/ [Accessed: 23- Mar- 2017].

44. "Proctor Exam | online Proctoring, " 2017. [Online].Available: https://proctorexam.com/ [Accessed: 23- Mar- 2017].

45. S.D. Patil and S.A. Patil, "Fingerprint recognition using minutia matching," World Journal of Science and Technology, vol .2(4), pp.178-181, 2012.

46. "U.are.U SDK, "2011. [Online].Available: http://www.crossmatch.com/Support/Reference-Material/Guides/SDK-Guides/Developer-Guide-2_0/ [Accessed: 23- Mar- 2017].

47. M. Lourde and D. Khosla, “Fingerprint Identification in Biometric SecuritySystems,” International Journal of Computer and Electrical Engineering, vol .2(5), p.852, 2010.

48. B.S. Bagepally, " Gaze Pattern on Spontaneous Human Face Perception: An Eye Tracker Study, " Journal of the Indian Academy of Applied Psychology, vol.41(3), p.127, 2015.

49. A. Dhingra, A. Kumar, M. Hanmandlu and B.K. Panigrahi, "Biometric Based Personal Authentication Using Eye Movement Tracking, " In International Conference on Swarm, Evolutionary and Memetic Computing ,pp. 248-256, 2013.

50. C. Merten and C. Conati, "Eye-tracking to model and adapt to user meta-cognition in intelligent learning environments," In Proceedings of the 11th international conference on intelligent user interfaces, pp. 39-46, 2006.

51. H.R. Chennamma and X. Yuan, "A survey on eye-gaze tracking techniques," arXiv preprint arXiv: 1312.6410, 2013.

52. "The eye tribe," 2017. [Online].Available: https://theeyetribe.com [Accessed: 23- Mar- 2017].

53. J. Kerkvliet and C.L. Sigmund, "Can we control cheating in the classroom?, " The Journal of Economic Education, vol. 30(4), pp.331-343, 1999.

54. B. Keresztury and L. Cser, “New cheating methods in the electronic teaching era," Procedia-Social and Behavioral Sciences, vol.93, pp.1516-1520, 2013.

55. S. Bob, "50+ Ways Schools ‘Cheat’ on Testing: Manipulating High-Stakes Exam Scores for Political Gain, " 2014. [Online].Available: http://fairtest.org/sites/default/files/Cheating50WaysSchoolsManipulateTestScores.pdf [Accessed: 23- Mar- 2017].

56. K. Yee and P. MacKown, "Detecting and preventing cheating during exams," PEDAGOGY, NOT POLICING, pp.141, 2009.

57. D. Faucher and S. Caves, "Academic dishonesty: Innovative cheating techniques and the detection and prevention of them, " Teaching and Learning in Nursing, vol.4 (2), pp.37-41, 2009.

58. Y.S. Chang and H.T. Cheng, “A scientific data extraction architecture using classified metadata, “The Journal of Supercomputing, vol.60 (3), pp.338-359, 2012.

Appendix

- **The Results of the Experiment in non-cheating status**

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1601	1st	717	19	483	529	11.67
	2nd	772	6	428		
	3rd	98	10	1102		
1602	1st	388	28	812	209.33	18.67
	2nd	149	16	1051		
	3rd	91	12	1109		
1603	1st	198	24	1002	271.67	22
	2nd	341	25	859		
	3rd	276	17	924		
1604	1st	180	18	1020	281.67	23
	2nd	346	25	854		
	3rd	319	26	881		

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1605	1st	255	27	945	233	22.67
	2nd	95	12	1105		
	3rd	349	29	851		
1606	1st	161	21	1039	156.67	19.67
	2nd	179	22	1021		
	3rd	130	16	1070		
1607	1st	7	1	1193	50.33	7
	2nd	62	9	1138		
	3rd	82	11	1118		
1608	1st	81	9	1119	41.33	5
	2nd	13	2	1187		
	3rd	30	4	1170		
1609	1st	399	40	801	370.67	34.33
	2nd	303	26	897		
	3rd	410	37	790		
1610	1st	123	14	1077	141	12
	2nd	159	10	1041		
	3rd	141	12	1059		

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1611	1st	16	2	1184	15.33	2.33
	2nd	4	1	1196		
	3rd	26	4	1174		
1612	1st	104	12	1096	135	13
	2nd	125	14	1075		
	3rd	176	13	1024		
1613	1st	161	12	1039	181.67	16
	2nd	209	22	991		
	3rd	175	14	1025		
1614	1st	35	5	1165	62.33	7.67
	2nd	7	1	1193		
	3rd	145	17	1055		
1615	1st	24	3	1176	220.67	17.67
	2nd	208	17	992		
	3rd	430	33	770		

- **The Results of the Experiment in cheating status**

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1601	1st	717	22	483	823.33	26.33
	2nd	863	32	337		
	3rd	890	25	310		
1602	1st	727	25	473	826.67	19
	2nd	738	21	462		
	3rd	1015	11	185		
1603	1st	906	21	294	866.67	20
	2nd	832	21	368		
	3rd	862	18	338		
1604	1st	1113	16	87	930.33	11
	2nd	791	8	409		
	3rd	887	9	313		
1605	1st	953	23	247	753.67	18
	2nd	745	16	455		
	3rd	563	15	637		

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1606	1st	1035	8	165	968	14
	2nd	985	20	215		
	3rd	884	14	316		
1607	1st	1117	13	83	932.33	10.33
	2nd	863	13	337		
	3rd	817	5	383		
1608	1st	1007	16	193	979.33	14
	2nd	1014	8	186		
	3rd	917	18	283		
1609	1st	1003	7	197	1076.33	6.33
	2nd	1164	4	36		
	3rd	1062	8	138		
1610	1st	1017	16	183	862	8.67
	2nd	740	4	460		
	3rd	829	6	371		
1611	1st	850	20	350	858.67	20.67
	2nd	853	11	347		
	3rd	873	31	327		

ID	Exam	The total time out of the screen (Second)	The number of times out of the screen	The total time in screen (Second)	The average time out of the screen (Second)	The average number of times out of the screen
1612	1st	1055	13	145	884	10
	2nd	911	9	289		
	3rd	686	8	514		
1613	1st	914	12	286	850.67	11
	2nd	870	10	330		
	3rd	768	11	432		
1614	1st	818	7	382	883	11
	2nd	841	12	359		
	3rd	990	14	210		
1615	1st	885	12	315	911.67	13.33
	2nd	940	16	260		
	3rd	910	12	290		

بـــــسم الله الرحـــــمن الرحـــــيم

﴿ وَمَا تَوْفِيقِي إِلا بِاللهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ ﴾ **سورة هود: آية 88**

نظام للكشف عن الغش في الامتحانات الإلكترونية

رزان حمزه باوارث

بحث مقدم لنيل درجة الماجستير في العلوم تخصص علوم حاسبات

د. عبدالله باسهيل
د. أنس فتوح
ا. د. شهاب جمال دين

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز
جدة – المملكة العربية السعودية
شعبان 1438هـ - مايو 2017م

نظام للكشف عن الغش في الامتحانات الإلكترونية

رزان حمزه باوارث

المستخلص

أدى التوسع في استخدام التكنولوجيا وشبكة الإنترنت خلال العشر السنوات الماضية إلى تزايد استخدام أنظمة التعليم الالكتروني بشكل غير مسبوق. تعتبر محاولة الغش في الاختبارات لظاهرة منتشرة في كافة أرجاء العالم بغض النظر عن مستوى تقدم البلد أو تطوره. كما أن استخدام الأدوات التقليدية لكشف عمليات الغش في الاختبارات الالكترونية لا تنجح في معظم الأحيان. تعتبر الاختبارات الالكترونية عبر شبكة الإنترنت جزءاً أساسياً ضمن أنظمة التعلم الالكتروني. حيث تقوم أنظمة التعلم الالكتروني بإدارة الاختبارات عن بُعد ومن دون وجود مراقبين فعليين. وكنتيجة لذلك، فإنه من السهولة بمكان محاولة الطلاب للغش خلال الاختبارات الالكترونية. تقوم الجامعات المقدمة لخدمات التعليم الالكتروني على اتخاذ إجراءات منها: إجراء عملية اختبار الطلاب بشكل تقليدي داخل الحرم الجامعي ، على الرغم من تناقض هذا الإجراء مع مفهوم التعلم الالكتروني. تناقش هذه الرسالة البحثية أساليب الحدّ من محاولة الطلاب للغش خلال الاختبارات المقدمة عن بُعد عن طريق: استخدام نظام تحقق مستمر من هوية الطالب حيث يضمن هذا الإجراء بأن الطالب المعني هو الذي يقوم بأداء الاختبار طوال فترة الاختبار كاملة ؛ وأيضاً عن طريق تفعيل نظام المراقبة الالكترونية عن بُعد ، والتي تساعد على كشف محاولات الطلاب للغش في الاختبارات المقدمة عن بُعد ومنعها. كما سنقوم في هذه الرسالة البحثية، بإنشاء نظام إدارة للاختبارات الالكترونية ، يستطيع القيام بالكشف عن محاولات الطلاب للغش في الاختبارات المقدمة عن بُعد. ينقسم العمل على هذه النظام على مرحلتين. المرحلة الأولى: وتتضمن مرحلة ما قبل قيام الطالب بأداء الاختبار عن بعد ، حيث يتم في هذه المرحلة استخدام نظام البصمة للتحقق من الطلاب المتقدمين للاختبار. تتضمن المرحلة الثانية قيام الطالب بأداء الاختبار، حيث تتطلب هذه المرحلة التحقق المستمر من أن الطالب هو نفسه المخول بأداء الاختبار. سيتم استخدام جهاز تعقب حركة العينين (Eye Tribe Tracker) خلال هذه المرحلة. وكنتيجة لذلك، فإنه سيكون باستطاعتنا التحقق من هوية الطالب المؤدي للاختبار، كما نستطيع معرفة ما إذا كان الطالب يقوم بمحاولة الغش خلال الاختبار عن طريق احتساب الوقت الذي كانت عيناه تنظران بعيداً عن الشاشة و عدد مرات ذلك.

الملخص

لقد أدى التوسع في استخدام التكنولوجيا وشبكة الإنترنت خلال العشر السنوات الماضية إلى تزايد استخدام أنظمة التعلم الالكتروني بشكل غير مسبوق. تعتبر محاولة الغش في الاختبارات ظاهرة منتشرة في كافة أرجاء العالم بغض النظر عن مستوى تقدم البلد أو تطوره. كما أن استخدام الأدوات التقليدية لكشف عمليات الغش في الاختبارات الالكترونية لا تنجح في معظم الأحيان.

في هذه الرسالة تمت دراسة أساليب الحدّ من محاولة الطلاب للغش خلال الاختبارات المقدمة عن بُعد عن طريق: استخدام نظام تحقق مستمر من هوية الطالب ؛ وأيضاً عن طريق تفعيل نظام المراقبة الالكترونية عن بُعد. ونتيجة لذلك، تم إنشاء نظام إدارة للاختبارات الالكترونية، الذي يستطيع القيام بالكشف عن محاولات الطلاب للغش في الاختبارات المقدمة عن بُعد.

تحتوي الرسالة على ستة فصول موزعة كما يلي:

1- **الفصل الأول:** يتضمن مقدمة عن موضوع الرسالة والتي تناقش:
   - أ- استعراض لخلفية موضوع الرسالة.
   - ب- أهميه البحث.
   - ت- أهداف البحث.
   - ث- نظرة عامة على الرسالة وكيفية تنظيمها في التوثيق.

2- **الفصل الثاني:** يقدم هذا الفصل الدراسات البحثية الحالية التي تجري من أجل حل مشكلة الأساليب التي يستخدمها الطلاب للغش في الامتحانات عن بعد وتضمن:

أ- مقدمة.

ب- الغش.

ت- التحقق بواسطة بصمة الاصبع وتعقب العين .

ث- أنظمة مراقب الامتحانات على الانترنت .

3- **الفصل الثالث:** يشرح نموذج اداره الاختبارات الالكترونية وتضمن الفصل:

أ- مقدمة.

ب- لمحة عامة عن الاختبارات وأنواعها.

ت- الطرق المستخدمة للغش في الاختبارات الإلكترونية والاختبارات عن بعد.

ث- التحقق المستمر من هوية الطالب بواسطة بصمة الاصبع وتعقب العين.

ج- مراقب الامتحانات على الانترنت في الاختبارات الالكترونية.

4- **الفصل الرابع:** عرض تنفيذ نموذج إدارة الاختبارات الالكترونية واحتوى على مرحلتين:

أ- مرحلة ما قبل قيام الطالب بأداء الاختبار عن بعد.

ب- مرحلة أثناء قيام الطالب بأداء الاختبار.

5- **الفصل الخامس:** تضمن النتائج والمناقشة للنتائج التي حصلنا عليها باستخدام النموذج المقترح.

6- **الفصل السادس:** ويحتوي على خاتمة البحث والأعمال المستقبلية.

نظام للكشف عن الغش في الامتحانات الإلكترونية

رزان حمزه باوارث

بحث مقدم لنيل درجة الماجستير في العلوم تخصص علوم حاسبات

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز - جدة
شعبان 1438هـ - مايو 2017م