A FRAMEWORK OF INTEGRATED CONTINUOUS ONLINE LEARNER WITH FUZZY NEURAL NETWORK APPLICATION IN LEARNING ENVIRONMENT

SITI FAIRUZ NURR BINTI SADIKAN

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

STATUS CONFIRMATION FOR DOCTORAL THESIS

A FRAMEWORK OF INTEGRATED CONTINUOUS ONLINE LEARNER WITH FUZZY NEURAL NETWORK APPLICATION IN LEARNING ENVIRONMENT

ACADEMIC SESSION: 2020/2021

I, **SITI FAIRUZ NURR BINTI SADIKAN**, agree to allow this Doctoral Research to be kept at the Library under the following terms:

1. This Doctoral Thesis is the property of the Universiti Tun Hussein Onn Malaysia.
2. The library has the right to make copies for educational purposes only.
3. The library is allowed to make copies of this report for educational exchange between higher educational institutions.
4. ** Please Mark (√)

□ CONFIDENTIAL (Contains information of high security or of great importance to Malaysia as STIPULATED under the OFFICIAL SECRET ACT 1972) *Title and Abstract Only*

□ RESTRICTED (Contains restricted information as determined by the Organisation/institution where research was conducted)- *Title, Abstract and Introduction Only*

□ EMBARGO ___________ until ___________
(date) (date)

☑ FREE ACCESS

Approved by

(SITI FAIRUZ NURR SADIKAN) (TS. DR. AZIZUL AZHAR RAMLI)

Permanent Address:

NO. 26-D, KG. PT. HJ. RASUL
MUKIM 4, 83000 BATU PAHAT
JOHOR

Date: 03 JUNE 2021 Date: 03 JUNE 2021

NOTE:

** If this Doctoral Thesis classified as CONFIDENTIAL or RESTRICTED, please attach the letter from the relevant authority/organization stating reasons and duration for such classifications.

This thesis has been examined on date 4 February 2021. and is sufficient in fulfilling the scope and quality for the purpose of awarding the Degree of Doctor of Philosophy.

Chairperson:

ASSOC PROF. TS DR. HAIRULNIZAM MAHDIN
Faculty of Computer Science and Information Technology
Tun Hussein Onn University of Malaysia

Examiners:

PROF. TS. DR. RUSLI HJ ABDULLAH
Faculty of Information and Communications Technology
Tun Hussein Onn University of Malaysia

PROF. DR. NAZRI MOHD NAWI
Faculty of Computer Science and Information Technology
Tun Hussein Onn University of Malaysia

A FRAMEWORK OF INTEGRATED CONTINUOUS ONLINE LEARNER WITH FUZZY NEURAL NETWORK APPLICATION IN LEARNING ENVIRONMENT

SITI FAIRUZ NURR BINTI SADIKAN

A thesis submitted in
fulfillment of the requirement for the award of the
Doctor of Philosophy of Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

JUNE 2021

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Student : ………………………………………
SITI FAIRUZ NURR BINTI SADIKAN

Date : 03 JUNE 2021

Supervisor : ………………………………………
TS. DR. AZIZUL AZHAR BIN RAMLI

Co Supervisor : ………………………………………
ASSOC PROF TS. DR. MOHD FARHAN MD.
FUDZEE

DEDICATION

I dedicate this thesis to Allah the Almighty, the cherisher and the sustainer who made my journey all worth it.

To my lovely parents, Siti Muhaia Binti Saib and Sadikan Bin Salijan, thanks for always being there for me. To my husband, Sulaiman Bin Mahzan, I appreciate your love and support. And for my little heroin, Anis Hadirah and little hero Hafiz Arif, I love you so much.

"THANK YOU for your endless support."

ACKNOWLEDGEMENT

Alhamdulillah, I am very grateful to Allah (SWT), whom with His willing and generosity, allowing me to complete my thesis. Firstly, my immeasurable appreciation and deepest gratitude to my supervisor, Ts. Dr. Azizul Azhar Bin Ramli and my co-supervisor Prof. Madya Ts. Dr. Mohd Farhan Md. Fudzee, for offering me their time, effort, help, support, advice, guidance, valuable comment, and suggestions in order for me to complete my thesis successfully.

My deepest thanks and appreciation to my lovely mother, husband and my family for their encouragement, their full support for me to study abroad and their prayer for ALLAH to grant me success in my study.

Thank you to all my friends; those who have been contributed in supporting my work, sharing important information about the study and assisted each other to complete this thesis. May ALLAH bless us all.

Finally, my thanks to Faculty of Computer and Information Technology (FSKTM) at University Tun Hussein Onn Malaysia (UTHM), for extraordinary commitment and cooperation during my study and for all lecturer who put their faith in me and encouraged me to give my very best.

ABSTRACT

Online learning has become popular among university due to its flexibility and adaptability. This technology offers the capability of learning, anytime and anywhere, based on student preferences. However, the general method of Personal Identification Number (pin) to verify the user does not guarantee a person's identity, because other people can use it. Even occasional visitors and users tend to pass their tokens or share their passwords with their colleagues to make their work easier. In all scenarios, online assessments such as quiz, test and examination are conducted without face-to-face supervisions. This situation potentially leads the students to find help from their peers or other sources to get high scores. This research addressed the issue related to the online assessment. The main objective of this work was to propose the use of the Online Learner Verification Framework (OLVF). This proposed solution utilizes the keystroke analysis and activity-based authentication for the online learner authentication. Besides, a fuzzy neural network approach was used to train and validate the learners' identity to predict their cheating tendency. In addition, challenge questions are also generated randomly by the system, based on user profiling. An online learning system was designed specifically in this study to simulate an original online learning assessment. It is expected to contribute to the field of security, where dynamic profile queries are asked, based on the previous history extracted from the online learning system. The proposed framework was validated using experimental datasets from an online learning system, elearning2u.com. The results obtained showed that, the proposed framework is able to overcome problems associated with the existing methods, thus improving the security level of the current online learning systems. Among others, appropriate questions and answers for the system-generated challenging questions are such that, invalid users will find them very difficult to guess. As a result, valid users too will find it difficult to provide their usernames and passwords to a third party or to ask others to answer online assessments for them. The results obtained proved this framework to be the safest method to be used, if implemented in the current online learning system.

ABSTRAK

Pembelajaran dalam talian semakin popular di universiti lantaran sifatnya yang fleksibel dan boleh disesuaikan dengan keperluan semasa. Ia berkemampuan untuk mempertingkatkan persekitaran pembelajaran pada bila-bila masa tanpa terbatas dengan geografi, mengikut kesesuaian pelajar itu sendiri. Secara umumnya, kaedah pengesahan capaian berdasarkan nombor pengenalan peribadi yang dimasukkan telah digunakan untuk proses pengesahan seseorang pelajar berkenaan. Namun, kaedah tersebut tidak sepenuhnya menjamin identiti seseorang pelajar berkenaan kerana ia juga mudah terdedah kepada penipuan. Nombor pengenalan peribadi atau kata laluan sebenarnya boleh diteka oleh rakan dan bahkan oleh pengunjung laman pembelajaran tersebut. Malah pelajar juga boleh sewenang-wenangnya menyerahkan ia kepada rakan semata-mata kerana ingin memudahkan kerja mereka. Kebiasaannya, tiada pemantauan secara bersemuka atau fizikal dilakukan semasa penilaian dalam talian seperti kuiz, ujian mahupun peperiksaan. Situasi sebegini membuka peluang kepada pelajar untuk melakukan pemalsuan identiti dengan mendapatkan pertolongan daripada orang lain untuk membolehkan mereka mendapatkan pencapaian atau markah penilaian yang lebih baik. Sehubungan itu, kajian ini dilakukan untuk menangani isu yang berkaitan dengan penilaian dalam talian. Objektif utama kajian ini adalah untuk mencadangkan penggunaan satu kerangka kerja untuk pengesahan identiti pelajar dalam talian atau 'Online Learner Verification Framework' (OVLF). Cadangan penyelesaian ini memanfaatkan kelebihan analisis ketukan kekunci dan juga pengesahan berdasarkan aktiviti pengguna bertujuan untuk mengesahkan capaian pelajar. Ia diperkukuhkan lagi dengan penggunaan Teknik Rangkaian Neural Kabur atau 'Fuzzy Neural Network' yang digunakan untuk melatih dan menilai data-data sehingga mendapatkan sesuatu paten identiti bagi seseorang pelajar, dan seterusnya ia digunakan untuk menjangkakan keinginan pelajar tersebut untuk meniru atau menipu. Kerangka kerja ini boleh dilaksanakan dalam mana-mana persekitaran pembelajaran dalam talian untuk mengesahkan identiti pelajar. Untuk itu, satu sistem pembelajaran dalam talian telah direka dan dibangunkan khusus sebagai satu plaform untuk membolehkan suatu penilaian pembelajaran yang sebenar dilaksanakan. Kajian ini menyumbang kepada bidang keselamatan siber kerana ia menggunakan pertanyaan secara dinamik mengenai diri pelajar berkenaan dan pertanyaan berkenaan adalah berdasarkan rentetan sejarah interaksi yang direkodkan di dalam sistem ini. Kerangka kerja yang dicadangkan ini telah disahkan dengan menggunakan set data daripada sistem pembelajaran dalam talian yang dibangunkan iaitu *elearning2u.com*. Hasil kajian membuktikan bahawa kerangka kerja yang dicadangkan berupaya meningkatkan tahap keselamatan pembelajaran dalam talian berbanding kaedah sebelum ini. Bahkan, ia menyulitkan orang lain untuk menjangkakan soalan dan jawapan daripada skema soalan cabaran. Sehubungan itu, pelajar tidak seharusnya mudah memberikan nama pengguna dan kata laluan kepada pihak lain atau meminta orang lain untuk menjawabkan soalan penilaian dalam talian bagi pihaknya. Maka, hasil kajian yang telah diperolehi menunjukkan bahawa kerangka kerja ini merupakan kaedah yang paling selamat sekiranya ia dilaksanakan dalam sistem pembelajaran dalam talian yang sebenar.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF SYMBOLS AND ABBREVIATIONS

ABA	-	Activity Based Authentication
ANN	-	Artificial Neural Network
F2F	-	Face to face
FAR	-	False Acceptance Rate
FCM	-	Fuzzy c-mean
FN		False Negative
FNN	-	Fuzzy Neural Network
FRR	-	False Rejection Rate
KDA	-	Keystroke Dynamic Authentication
MLP	-	Multilayer Perceptron
MSE	-	Mean Squared Error
NN	-	Neural Network
PBA	-	Password Based Authentication
SD	-	Standard Deviation
SME	-	Subject matter expert
TP	-	True Positive

LIST OF APPENDICES

LIST OF PUBLICATIONS

Journals:

(i) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md Fudzee, Siti Sapura Jailani, Mohd Ali Mohd Isa, Prasanna Ramakrisnan (2019) "User Behaviour Pattern for Online Learning System: UiTM iLearn Portal Case." Indonesian Journal of Electrical Engineering and Computer Science. Vol. 10, No. 1, pp. 382-390

(ii) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md Fudzee, (2019) "An Initial Framework of Fuzzy Neural Network Approach for Online Learner Verification Process" International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, No. 13, pp. 185-189.

Proceedings:

(i) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md Fudzee. "A Survey Paper on Keystroke Dynamics Authentication for Current Applications". AIP Conference Proceedings, Vol 2173, Issue 1, pp. 020010-1, 020010-11.

(ii) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md Fudzee, Mohd Helmy Wahab. "An Initial Framework of Hybrid Neuro Fuzzy Approach for Online Learner Verification Process." Proceeding in The International Conference on Advanced Science, Engineering and Information Technology 2011 (ICASEIT 2011), pp. 178-184, Adya Hotel, Langkawi, Malaysia, 14-15 January 2011.

(iii) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms through Fuzzy Neural Network Algorithm", Proceeding in Academic International Dialogue Conference (AID 2011), pp. 147-150, Universiti Sains Islam Malaysia, 20 November 2019.

(iv) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. “e-Cheater’s Detection System (e-CDS)”, Proceeding in Academic International Dialogue Conference (AID 2011), pp. 27-30, Universiti Sains Islam Malaysia, 20 November 2019.

(v) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. “An Integrated Continuous Online Learner Verification Framework using Fuzzy Neural Network”, Proceeding in Academic International Dialogue Conference (AID 2011), pp. 147-150, Universiti Sains Islam Malaysia, 20 November 2019..

Conference Presentations:

(i) **S**iti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Shahreen Kasim, Hairulnizam Mahdin, Mohamad Aizi Salamat, Untari Novia Wisesty. “An Initial Framework of Fuzzy Neural Network Approach for Online Learner Verification Process”, 5th International Research and Innovation Summit (IRIS5). Adya Hotel, Langkawi, Malaysia. 7 -8 December 2017.

(ii) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Mohd Helmy Abd Wahab. “Fuzzy C-Mean Clustering: User Behaviour Profiling for Online Learning System”. The 5th International Conference on Communication, Management and Information Technology (ICCMIT). Vienna, Austria. 26-28 March 2019.

(iii) Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee. “A Survey Paper on Keystroke Dynamics Authentication for Current Applications”. International Conference on Electrical and Electronic Engineering 2019 (ICon3E). Everly Hotel, Putrajaya, Malaysia. 24-25 June 2019.

LIST OF AWARDS

(i) **3rd Grand Prize Award in Asia International Innovation Exhibition [AIINEX 2020]:**
Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah, Mohd Helmy Abd Wahab. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(ii) **1st Special Award in Asia International Innovation Exhibition [AIINEX 2020]:**
Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah, Mohd Helmy Abd Wahab. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(iii) **Gold Award in Asia International Innovation Exhibition [AIINEX 2020]:**
Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah, Mohd Helmy Abd Wahab. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(iv) **Silver Award in Asia International Innovation Exhibition [AIINEX 2020]:**
Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah, Mohd Helmy Abd Wahab "e-Cheater's Detection System"

(v) **Gold Award in International Research and Innovation Symposium & Exposition [RISE 2020]:**
Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Helmy Abd Wahab. "Online Learning System with Authentication & Identifiation Mechanism Using Fuzzy Neural Network Version 2.0"

(vi) **Special Award "Double Gold" in International Science and Social Science Innovation Competition [i-SIC 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms through Fuzzy Neural Network Algorithm"

(vii) **Gold Award in International Science and Social Science Innovation Competition [i-SIC 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms through Fuzzy Neural Network Algorithm"

(viii) **Gold Award in International Science and Social Science Innovation Competition [i-SIC 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "e-Cheater's Detection System"

(ix) **Silver Award in International Science and Social Science Innovation Competition [i-SIC 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Harun Shahudin. "e-Learning2u"

(x) **Bronze Award in International Science and Social Science Innovation Competition [i-SIC 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "An Integrated Continuous Online Learner Verification Framework Using Fuzzy Neural Network"

(xi) **Gold Award in International Invention & Innovative Competition (InIIC Series 2/2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "e-Cheater's Detection System"

(xii) **Silver Award in International Invention & Innovative Competition (InIIC Series 2/2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(xiii) **Gold Award in Breakthrough Invention, Innovation and Design Exhibition [BiiDE 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "e-Cheater's Detection System"

(xiv) **Gold Award in Breakthrough Invention, Innovation and Design Exhibition [BiiDE 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(xv) **Gold Award in National Innovation & Invention Competition [NIICe 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "Online Learning System with authentication and Identification Mechanisms Using Neuro-Fuzzy Algorithm"

(xvi) **Gold Award in National Innovation & Invention Competition [NIICe 2019]:**

Siti Fairuz Nurr Sadikan, Azizul Azhar Ramli, Mohd Farhan Md. Fudzee, Sulaiman Mahzan, Mohd Ab Malek Md Shah. "e-Cheater's Detection System"

CHAPTER 1

INTRODUCTION

1.1 An Overview

Online learning is become more popular among university due to its flexibility and adaptability. A fully online learning, blended learning, and a learning which integrate online and face-to-face instruction, seem to be growing (Swan, 2019). This technology has capabilities for learning anytime and anywhere to improving an online learning environment based on student preferences. It involves the training, delivery of knowledge and motivates students to interact with each other, as well as exchange and respect different point of views (Arkorful & Abaidoo, 2014).

Some examples of online learning system implemented in Malaysian University are Multimedia Learning System (MMLS), and i-Learn. Both MMLS and i-Learn are a multifaceted system which facilitates the management of course content. It also facilitates asynchronous communication such as online test and grading and enables students to be monitored in the forum and other assessment tasks. According to Fedynich, Bradley, & Bradley (2015), 93.17% of graduate students universities are generally positive about their experiences with online courses.

However, online learning has some limitation (Sadeghi, 2019), including the security of online assessment such as quiz, test and examination. Practically, it is often easier to cheat online (Moten, Fitterer, Brazier, Leonard, & Brown, 2013) since the assessments such as online quiz and test which are less monitored, and assessment can often be done at any time of day (Gilbert, 2015). Besides, students often have less commitment to the integrity of online learning programs compared to face-to-face or classroom learning environment (Michael & Williams, 2013). This situation may lead to unfair evaluation if most of the students cheating on their assessment (Melaka, 2020). This thesis investigates the usability and security of authentication in online learning assessment.

1.2 Research Background

The learners' environment on online learning integrated with security and dependability interrelates with trust, as dependability is a subjective and reflects the learners' degree of trust towards the system (Sheila, Faizal, & Shahrin, 2014; Paullet & Douglas, 2014). For instance, Personal Identification Number (PIN) is one of the verification methods that are based on properties that can be forgotten, disclosed, lost, or stolen. Another example is passwords that are easily accessible as users tend to pass their tokens with their colleagues in certain circumstances (Matyas & Riha, 2002). Thus, these situations lead to the online cheating situation.

Even the best students may become tempted to cheat due to pressures to succeed or to avoid the stigma of failing can drive the most ethical child to choose the easy path. A lot of student cheat, but just by a little depends on the situation. Some students tend to cheat when there is not much time to complete an assessment, and when the task is too boring, irrelevant or difficult. While cheating may occur in any online assessment, cheating in exams is a more significant problem, since it is the universal benchmark method of assessment in all the global higher educational systems (Starovoytova, 2016). However, the number of students who were cheating in exam increases every year.

Based on a survey conducted in Canada, more than 7000 students have been involved in academic misconduct resulting in the discipline in academic. According to the authors, the number of university students who cheated has increased by 42% by using smartphones and other devices, specifically for cheating. This cheating scandal can also damage the reputations of the university. Meanwhile, Mustapha & Ali (2017) stated that 57.4% of Malaysian students in major public universities admitted to having participated in academic dishonesty at least once in their study.

Besides, 54% of the students disagreed that cheating is difficult on online assessment, whereas only 33% agreed (Ozden, Erturk, & Sanli, 2004). Besides, a study regarding cheating online reported that 72.5% of students reported cheating when taking online quizzes and exams (Loschiavo & Shatz, 2011). In the other hand, nearly

74% of students indicate that it would be somewhat easy to cheat in online exams, and about 29% of the students admitted to cheating in online exams. In addition, over 50% of students willing to cheat if the risk of detection is low (Rigby et. al., 2015). On January 2, 2016, The Times reported almost 50,000 students at British university had been caught cheating in the past three years amid fears of a plagiarism "epidemic" fueled disproportionately by foreign students.

In the other hand, some websites offer to complete all aspects of the course to students, including assignments and examinations. These entrepreneurs and freelancers provide services to take entire online classes and complete the assessment for their client, online. The services also include online class help, online test services, essay writing services and discussion board (Reynolds-Seraphin & Collins, 2017). The purchased assignment can be cheap, with the average freelancer academic can be purchased at USD 101 (Clarke & Lancaster, 2013), and it can be of high quality. The Times Higher Education on September 10, 2016, reported that the contract cheating sites presenting their offer as legitimate. This situation will promote online cheating among students. Thus, in order to prevent the cheating on online assessment, a higher level of security is needed especially with identifying the correct person log to the system. However, as the security level is applied to this online learning, it will impact the accessibility towards the overall of the system.

In addition, online learning depends on the internet and network for running the services. However, there are numbers of illegal activities and security threats taking place on the Internet and network. Consequently, the nature of the online learning environment is inevitably exposed to constant security threats, risks, and attacks. Since online learning takes place via the internet and network, every element in an online learning system can be a potential target of hacking or attack. The common authentication and access control attacks are dictionary attacks, brute force attacks, spoofed logon screen, and sniffer. The dictionary attacks are programs with built in dictionaries where the attackers use all dictionary words to attempt and find the correct password, in the hope that a user would have used a standard dictionary word.

Meanwhile, brute force attacks are attempting to break the password by trying all possible words, in the alphabet and attempt all possible combinations including special keywords. In the other hand, the spoofed logon screens are attacked to implement a fake logon screen, and when a user attempts to login, the logon screen will send the username and password to the hacker. While sniffer attack is access control occurs when attackers' use sniffer to capture information transmitted over a network including passwords which can be captured and read by the program.

The technology does not disrupt the user's session, but a masquerader who hijack the session such as when the user is away from the keyboard (Killourhy & Maxion, 2012). This situation may lead to unauthorized and destruction of content and its educational source such as malicious attack for higher grades (Ullah et. al., 2012) and get the best result in a simple way by replacing or changing their score. Besides, the conventional Password-Based Authentication (PBA) systems are vulnerable to password attack (Shaker *et al.*, 2014). In another case, anyone can access their online assessment with bad intention if the initial user does not properly log out or the user leaves the system unattended to take a short break without logging out (Agashe & Nimbhorkar, 2015). In order to resolve the problem mentioned, the system must continuously monitor the user as well as to authenticate the user at the initial login session.

Then, a new mechanism should be applied to this online learning in order to improve the security level along with the login session. However, the issue of current login method is that only authenticate user at the initial login and do not re-authenticate user until the user log out from the system (Agashe & Nimbhorkar, 2015). In this scenario anyone can access the system resources and cheating as discussed in the previous paragraph. Several studies have proposed an advanced authentication mechanism that can provide continuous authentication to the user by using biometric. Biometric is referring to the automatic identification of a person based on physiological or behavioral. The physiological type includes biometrics based on body traits such as fingerprint, face, iris, and hand and it is considered to be more robust and secure. However, it also considered to be more intrusive and expensive and require a special hardware. On the other hand, examples of behavioral biometric are voice, signature, lip movement, mouse dynamic, and keystroke dynamic which include any learned movement. Based on the previous study, keystroke dynamics is the most popular method, because it only requires a keyboard with no extra devices (Sawant, Nagargoje, Bora, Shelke, & Borate, 2013). Thus, even if the user knows the username and password, these keystroke dynamics can be considered as the best tools to secure systems.

1.3 Problem Statements

Keystroke dynamic has been highlighted as an alternative to securing password (Singh *et al.*, 2017; Patil & Renke, 2016). Its cheap implementation is a good factor to make it user-friendly (Shaker et al., 2014a). Besides, it can be used over the internet and does not need training for end user. This keystroke dynamic can be combined with password-based authentication to achieve strong authentication. It can be constructed from various typing features such as typing speed, the duration between the successive key pressed, the pressure applied on the keys, and finger position on the keys.

Moreover, it is very easy to capture data as keyboards are common and no special equipment is necessary (Ali et. al, 2017). Keystroke dynamics also is economical and can be easily integrated into the existing computer security systems with minimal alteration and user intervention (Nagoriya et. al., 2020). Besides, keystroke dynamics proved most appropriate for continuous authentication (Deutschmann, Nordstrom, & Nilsson, 2013). The previous keystroke framework have been proposed by Kang & Cho (2015) and Karnan, Akila, & Kalamani, (2009) for identity verification. These frameworks used both proved useful in illuminating different aspects of features to achieve high accuracy and strong authentication.

However, the keystroke dynamic, which is based on the individual's typing pattern, may also vary depending upon the application in use. A user participating in the chat session may type fairly release style, while the same user may type in a significantly different way when producing a document. There is a category of user use numeric keypad when entering a large number, especially the registered course involves mathematic and calculation. The injury, fatigue, or distraction might result in variation of typing rhythm (The et. al., 2013). Besides, casual typing, using single hand for entering the password, sweaty hand after a long session and the keyboard layout also can lead inconsistency in the typing style (Sawant et al., 2013). In the other hand, the different activity along the semester which depends on registered courses and the types of assessment might affect on the keystroke analysis result. This scenario will produce a different result of typing rhythm and make the authentication result failed and lower accuracy. Thus, enhance security is needed.

There is a various analysis method of keystrokes dynamics such as statistical, data mining, and neural network. According to Vinayakvitthal & Charniya (2015) keystroke dynamic analysis method can be broadly categorized into the statistical approach and machine learning approach. The previous studies have primarily concentrated statistical approach was mostly applied for static keystroke analysis. Besides, the other machine learning algorithm should be tested to improve the accuracy of this keystroke (Kang & Cho, 2015). In comparison, the machine learning approach is used to classify and identify a pattern and make the correct conclusion based on the provided data. A neural network is widely studied to be capable of learning nonlinear models of data. Recently, various artificial neural networks (ANNs) have been applied to the keystroke classification problem, including multilayer perceptron, backpropagation neural network, and Art-2 neural network (Abisado et al., 2017; Wankhede & Verma, 2014; Harun et al., 2010) due to the ability to recognize complex noisy patterns. However, it has the limitations that restrict them as a substitute for traditional methods such as statistical regression, pattern recognition and time series analysis.

Neural networks, however, require a substantial amount of data to train on, before they can successfully classify incoming data. Due to this limitation, the neural network is not able to train well, resulting in their lower detection accuracy (S.Shraddha, 2014). The different hybrid approaches have been explored in the past to overcome the drawbacks of any one particular method. ANN and Fuzzy clustering are used so that it complements to each other which neural networks are good at being able to classify unseen data points. In contrast, fuzzy clustering enables the algorithm to generalize well (Trivedi, 2014). By combining neural network and fuzzy logic, the performance of the system is improved. In recent years, there has been an increasing interest in fuzzy neural network approach for other application such as credit card fraud detection and intrusion detection system. However, there is a lack of research in fuzzy neural network approach for continuous user authentication. Therefore, an integrated authentication framework in verifying online learner identity using fuzzy neural network approach is developed to improve the level of security in the current online learning environment.

Kang & Cho (2015) also proposed the use of an authentication method independent of the input device or an integrated KDA framework incorporating all input devices should be design for future work. This would help to eliminate the need for users to change input devices that could use to connect to the online system. Then, this study would integrate the KDA with activity-based authentication (ABA) with incorporating any input devices and platform. This ABA is implemented due to ability that activity browsing histories are not simply copied or pass to others and there is no special credentials are essential (Bailey, Okolica, & Peterson, 2014). Then, the challenge question based on the activity browsing histories extracted and act as mechanism for verification of this ABA. The information such as score mark, total post and date from online learning system is used to individually verify them by comparing the answer by the user and answer stored in the database. However, the generation of this challenge question is solely depending on the presence of cheating tendency. This cheating tendency is used as a determinant factor toward challenge question for the ABA.

1.4 Purpose of the Study

The purpose of this mixed method research is to propose the use of Online Learner Verification Framework (OLVF) for enhancement to the current framework for keystroke authentication by combining with activity-based authentication using challenge question and cheating tendency as to the mechanism for verification and the consideration of cheating tendency to verify user identities in online learning system with highest accuracy and efficiency. This research uses mixed method study that engage in integrated authentication framework. The qualitative phase of this study examined user's behavior which were influenced by several factor for prediction their cheating tendency. Besides, the quantitative phase of this study further examined the readiness, and activity pattern of user.

1.5 Scope of the Study

The research is focusing on enhancing the current working frameworks proposed by Kang & Cho (2015) and integrates it with the framework by Karnan, Akila, & Kalamani, (2009) for identity verification. This framework is used as a mechanism for better security in an online learning environment. In this research, user profiling is implemented to track the pattern of learner's activity for online learner identity verification. The technique used in the case study to recognize user behavior on online learning is web mining. Besides, this research was only focusing on user's online activity during the logged session by recording their keystroke to investigate user profile characteristics and cheating tendency using fuzzy neural network. Meanwhile, activity-based authentication only focusing on network activities where the challenge question will be generated based on browsing history with the presence of cheating tendency. The performance metric of the proposed framework and the existing were compared and analyzed, based on MSE and MAPE using fuzzy c-mean (FCM), neural network (NN) and fuzzy neural network (FNN).

1.6 Objectives of the Study

This research aims the specific goal to achieve several objectives:

(i) To enhance an integrated continuous online learner verification framework using the combination of password-based authentication, keystroke-based authentication and activity-based authentication, taking cheating tendency into consideration in verifying online user's identity for better performance in the online learning system.

(ii) To develop an integrated continuous authentication framework for learning environment (as produce in (i)) in verifying online user's identity using fuzzy neural network application.

(iii) To evaluate the performance of the proposed approach against other methods by using a performance metric, based on MSE and MAPE.

1.7 Research Questions

This thesis aims to answer the following research question as follows:

(i) How to enhance an integrated continuous Online Learner Verification Framework (OLVF) using the combination of password-based authentication, keystroke-based authentication and activity-based authentication with the consideration of cheating tendency be used in verifying online user's identity for better performance in the online learning system?

(ii) How can the framework approach using fuzzy neural network be used for verifying online user’s identity in the online learning system?

(iii) How is the performance of the proposed framework in verifying online user’s identity in the online learning system?

a. How is the performance of keystroke dynamic authentication in proposed framework for verifying online user’s identity in the online learning system?

b. How is the performance of cheating tendency in proposed framework for verifying online user’s identity in the online learning system?

c. How is the performance of activity-based authentication in proposed framework for verifying online user’s identity in the online learning system?

1.8 Significance of the Study

The study proposed an integrated authentication approach that tracks the pattern of learner's activity through user behavior-based password, keystroke and activity-based authentication. This approach helps the administrator in the evaluation of tests and assignment of the grades to the students. These data techniques can be used in any learning system for tracking student behavior during the process of online learning.

Besides, this research could give various significances especially to the targeted user. First, users can get use any platform for online learning including personal computer, mobile and other devices. This research also gives benefits to the lecturer or an educator to verify the learner whether they are the correct user or not, due to lack of implementation method for verifying the correct student to log on to the system in the current online learning system. The proposed framework can be used and implement in any online learning system for various platforms and devices like desktop and mobile phone. Besides, it will provide a new trend in securing online learning system for student and lecturer.

1.9 Outline of the Thesis

This thesis is organized into seven (7) chapters, namely, introduction, literature review, research methodology, user behaviour on online learning, system analysis and design, simulation results and analysis, and lastly conclusions and recommended future work.

Chapter 1 presents an introduction to this research, where the research background and problem statement were introduced in the context of this research. Besides, the aims, objective, scope of this research were identified. In order to provide the rationale for this research, a relevant literature review was conducted and presented in the following chapter.

Chapter 2 provides an extensive review of online learning, information security, authentication, and usability of authentication methods, which explains the rationale and the basis for this thesis. This chapter also explores information security with a focus on threats for online assessments and others. Besides, the methods, techniques and studies in this thesis are reviewed and discussed in detailed. This was done to justify the reasons for implementing each technique and method.

Chapter 3 gives a brief explanation of the overall methodology of the research. The framework that depicts the whole flow of this research is presented to provide a general view of the way the research is accomplished. In this chapter, the process involved in the configuration of challenge questions, together with an algorithm for generating these challenge questions and activity-based authentication is also presented. Other phases of the research are also briefly explained and further descriptions about these phases will be continued in the subsequent chapters of this thesis.

Chapter 4 presents the case study analysis for user behaviour in online learning. The case study is divided into three sections, namely, readiness, activity and user pattern behaviour. The study of user pattern behaviour focused on the analysis of the web server log file data of the online learning system to gain the navigational pattern of the online learning user. The study of the online user behaviour while navigating online sites is an important issue to have a clear understanding of the problem. The case study also can help to improve the security of online learning, especially during the assessment progress, such as online quizzes, tests and examinations. The framework for user navigation is implemented in this research for clustering purposes to get a pattern of learner's activity.

Chapter 5 presents the development and the integration prototype of online learning systems. The configuration of keystroke dynamic authentication, cheating tendency and challenge questions used in this research is also reviewed and discussed, to get a clear view of the implementation of the research study. In the following chapter, the simulation results and analysis of the adapted methods and techniques for this research will be further discoursed.

Chapter 6 reveals the findings and results obtained from the investigation of integrated authentication system. The results for user cheating tendency and keystroke analysis using neural network, fuzzy c-mean and fuzzy neural network are presented. This chapter also summarises the presented framework for the integrated authentication system. Besides, performance comparison with other technique is also presented.

Chapter 7 presents the conclusions and recommended future work. This research concludes its findings and results to reflect its main purpose in this chapter. The contributions of this research are pointed out, while the recommended future work is also discussed to extend this research further.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the work of literature related to this research. The techniques and methodology applied for the research are instigated from topics discussed in this chapter. Literature review in this chapter comprises discussions on online learning, security, user authentication, keystroke dynamic authentication, artificial neural networks, fuzzy logic, fuzzy neural network, user cheating tendency, and other subjects that are related to this research.

2.2 Online Learning

The concept of online learning has been discussing in literature with multiple term and definition. Researcher and practitioners have referred to online learning, e-learning, distance learning, blended learning and hybrid learning sometimes seem to be used interchangeably. Online learning is commonly defined in contradistinction to face to face learning (Ryan et al., 2016). It uses web-based technologies which offering opportunities for out-of-class learning independent of time, place and pace. In other words, online learning is a computer-based educational tool or system that enables the user to learn anywhere and at any time (Epignosis, 2014).

According to Doe, Castillo, & Musyoka (2017), there is no consensus on the term for this mode of learning where its variations include distance education, online classes, and online learning. In addition, these type of learning or teaching is sometimes known as hybrid; incorporating a synchronous, with some asynchronous meetings. There have also been increases in demand for online learning from students from all walks of life (Nguyen, 2015). Online education offers flexibility, affordability, and portability; especially to a population who otherwise would not get the opportunity to earn a degree and others certificate.

The reason why there is so much discussion on online learning in previous literature is that there are a lot of benefits and uses of online learning. Some of the most important things are its effectiveness in educating students, its use as professional development, its cost-effectiveness. It also offers access to online resources, databases, periodicals, journals and other material user would not usually have access to from a library (Epignosis, 2014). This opportunity allows the student to have immediate access to supplementary, unlimited and mostly free material online which also can potentially maximize the time spent learning rather than looking for information. Besides, it able to provide opportunities for relations between learners by using discussion forums (Arkorful & Abaidoo, 2014). So that it can help eliminate barriers that have the potential of hindering participation including the fear of talking to other learners. Thus, it motivates students to interact with others, as well as exchange and respect different point of views.

2.2.1 Online Learning Assessment

The use of online learning assessment or e-assessment has increased in higher education over the last two decades (Boitshwarelo, Reedy, & Billany, 2017). It helps the educational institutions to monitor their students and keep eyes on their progress (Hameed & Abdullatif, 2017). It allows the student to take their assessment without attending the traditional classes due to their life circumstances. It can save much time by gives a quick result to the students. The student can also take the assessment anywhere and anytime as long as there is an internet connection. The student also can submit their assignment and tasks given by lecturer at any time. Besides, online assessment requirement makes it easy for lecturers to conduct and evaluate the exam in a short time. Besides, online assessment is also more reliable and cheaper.

There are many types of online learning assessment such as online quiz, online assignment, online test and online examination. In online learning, the online examination is the most important component (Younis & Hussein, 2015). The purpose of online examination systems is to take online exams efficiently and save a timeconsuming in checking, marking, return the paper (Younis & Hussein, 2015). The main objective of online examination is efficiently evaluating the candidate fairly through a system.

2.2.2 The Threat of Online Learning

Online learning security plays an important role in any online learning systems development. There are many challenges faced by learners, online learning provider and Higher learning Institutions as discussed by other researchers. According to Adetoba B. T., (2016), these challenges are interoperability of applications, standardization and compatibility, the security policy with enforcement mechanism and online learning infrastructure.

The interoperability of applications challenges is an emerging trend which demanding a higher level of interoperability for components, applications, systems, together with environments which are often developed for certain institutions or organization and provide very similar functionalities. In contrast, standardization and compatibility are vital for both online learning service providers and learners to be able to interchange components. These are very important where different online learning systems must interact with other online learning.

Besides, security policy and enforcement mechanism are defined as the set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information. Then, it must be captured and followed at application runtime via an enforcement mechanism which represents the set of centralized and distributes software to ensure that the security policy is maintained and never violated. In the other hand, online learning infrastructure refers to software, hardware and connectivity required for online learning development and implementation.

In other research by Adetoba B. T. (2016), the possible threat to online learning system and countermeasures can be summarized into six (6) categories which are availability, integrity, confidentiality, authentication, and authorization. Availability threat is a threat that occurs when services of a system and contents are unavailable to legitimate users for some time. In comparison, integrity threat is a threat that aims to destroy or modify the contents of the system. In the other hand, authentication threat is to gain access to system information by using stolen passwords, key or credentials or an attack device pretending as legitimate device trying to gain access to the system. Authorization threat is a threat that occurs as a result of unauthorized access to specific content.

However, this research is only focusing on confidentiality threat. This threat tries to expose confidential data to unauthorized users. These studies indicate that the current authentication approach in online learning cause many threats and thus create opportunities for their legitimate learner or student or user to cheat. The legitimate learner may collude with the third party, who impersonate them in their online assessment such as quiz, test and examination. In addition, this learner maybe transfers the online learning contents to the unauthorized persons or another person. In other words, this learner tends to pass their tokens, such as passwords that are easily accessible with their colleagues in certain circumstances (Matyas & Riha, 2002).

2.2.3 Factors for Cheating in Online Learning

There are several factors that make students cheat in online learning assessment. The main factors for cheating included laziness, wanting to achieve higher grades, and pressures to succeed (Radulovic & Uys, 2019). Other factors like education level, age, mode of study and education of father have a very important role in the motivation of cheating according to the regression logistic analysis Wang *et al.*, (2015). The factors for cheating can also be direct responses to people, hard materials, and teacher indifferences and at the end of a serious failure to lack of student's study noted. Some of lecturers and educators are using the same questions which enable their students to upload the questions in the Quizlet app, which can encourage students to cheat too. Other than that, the test monitoring and management system are not sufficient enough, making it easier to cheat in an online learning assessment. Furthermore, the examination paper and examination questions make cheating possible may it be online or offline if the student has an intention to cheat during that time.

Table 2.1 shows the Top 5 reasons for test cheating which are no time to prepare test but want to pass the exam; others cheat, so do I. Otherwise is unfair; my friend wants me to help him//her; need a higher score for honours, study abroad, keep leadership; and prove my skills in information technology, I cheat, no one finds out.

Table 2.1: Top five reason for test cheating

Possible Reason	Rank	Numbers of agreement
No time to prepare test but want to pass the exam	1	97
Others cheat, so do I. Otherwise is unfair	2	70
My friend wants me to help him//her	3	46
Need a higher score for honors, study abroad, keep leadership	4	32
Prove my skills in information technology, I cheat, no one find out	5	23

The top reason for cheating is no time to prepare a test but want to pass the exam; in other words, fear to fail. This show that if the students lack preparations, means students do not prepare their exam perfectly (C. Loschiavo, 2017) make them pressure to succeed. The fear of failure is a by-product of the pressure to succeed; hence the two motives are directly related (Radulovic & Uys, 2019). However, the students should prepare mentally and physically before the examination day. Then the students can build up their confidence level to answer all question (Madara, 2016).

The second reason for cheating is 'others cheat, so do I. Otherwise is unfair'. This reason happened because of peer influence. Peer influence is the most factor that may affect the behavior of a teenager. One of the causes from peer influence is some of their friends cheat during an online exam and get a good result, which influent them to do the same. Besides, this student asks other help to answer questions online within the prescribed time (Bemmel, 2014). This situation will negatively affect the other student, which they might be doing the same thing as the previous students do (Madara, 2016). Thus, make cheating is common among universities students.

The other reason is that my friend wants me to help him//her and need a higher score for honours, study abroad, keep the leadership. Sometimes, these student cheating, due to lack of confident level, gets scored in the examination. They are cheating in examination in order to build the self-confidence to get scored. Test results are shown in the classroom also make the students feel lower confident (Muchai, 2014). The level of self-confidence is a must for all students to be brave to stand out.

Meanwhile, the lack of monitoring in the online examination may result in students are more likely to cheat in online courses. Student often not monitored in the online examination and free to share answers for exams, at home, or in any environment which provides internet access (Bemmel, 2014). This is because of the internet facilities are no boundaries which makes it challenging to monitor among students when answering the online examination. Therefore, this situation encourages the student to take a shortcut by doing cheating during exam.

2.2.4 Cheating Technique in Online Learning

An examination or assessment is important to any educational program, and online learning is no exemption. In any exam, there is a possibility of cheating, and therefore, its detection and prevention are important (Atoum, Chen, Liu, Hsu, & Liu, 2017). There are many ways students cheating in online examinations. One of the methods usually done by students is hiring other people or freelancer to answer their online exam. Nowadays, the freelancers are openly advertising their services to help students cheat in their online examinations (New, 2015). These online cheaters will take on the student's identities and take entire online classes and examination. The student uses this alternative because of their lazy attitude but wants to get a good grade. According to Bemmel (2014), 0.7% asked others to take their online exam for them.

Another way to cheating online in the examination is to create multiple identities. This is a new technique of cheating that emerges in Massive Open Online Courses (MOOCs). The technique is called CAMEO, which means Copying Answer using Multiple Existences Online. The research has identified that this technique is exploited by the ability to create "multiple personalities" in online courses. To get a good result, the student will register to the courses more than one identity, the first one which is the fake identity that they register is a "harvester" which mean they use as a guess-and-check-strategies to gather the correct answers. The other identity is a "master" for them to submit the correct answer.

2.2.5 Existing Authentication Approaches

Nowadays, several applications can be used to prevent online cheating in examination. Firstly, by using *the Respondus LockDown Browser*. This program is a special browser that guarantees the testing environment as it prevents students from copying and pasting text, go to another URL or opening other webpages and taking screenshots while taking online test or examination. Lecturer or course administrator can use the *Respondus Monitor* to record video and audio of the test takers during the examination.

Then, the course administrators can confirm the identity of the students and act as a great barrier to cheat. Besides, the student needs to use LockDown Browser and there are not allowed to use others browser. Even though this method prevents online exam fraud, this method is still imperfect where the student can still cheat during their online exams with the help of other technologies.

Recent research has shown that biometric is becoming a principal method of securing any online system (Adetoba B. T., 2016) specifically online learning. The use of biometrics can support the security control, authentication and integrity of online exam process. It will check the students from the database which is collected and stored in the registration process. The students will be given specific permissions like reading and writing for the specific time. The students who enter from the different IP's cannot use the allocated domain, and thus the system is secure. *Proctortrack* can be used for exam monitoring services that are anti-cheating software technology. It is used to verify students' identity with facial recognition, ID card and knuckle over a webcam. It enables the course administrator to watch the face and computer screen of the students as they take the test. A red alert band on the computer screen will appear indicating that the program is recording video and monitoring the students as the exam begins. To make sure he is reminded that he is being watched, the *Proctortrack* also shows an image directly in the miniature on the screen. In addition, lighting changes can also result in test to flag for a violation and even stretching, looking away, or leaning down to pick up pencil could flag the student's test (Natasha Singer, 2015). Figure 2.1 shows an example of students on Proctortrack

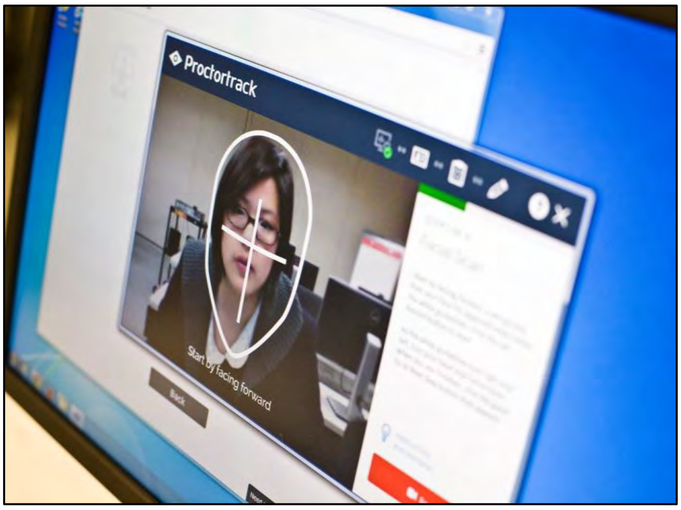

Figure 2.1: An example of students on Proctortrack

The use of *Proctortrack* is not mandatory, and face-to-face traditional proctoring has become an acceptable alternative over time. Moreover, *Proctortrack* prevents the students from receiving any assistance such as textbooks, notes, friends and unauthorized devices with continued verification throughout the exam. It also restricts certain application and keystrokes to prevent students from cheating. It is a good approach to avoid cheating during the online examination. There are many other tools used that perform the same functionality as *Proctortrack*, which monitors students taking online tests like *ProctorU, Faronics Insides, SafeBrowser, and ExamSoft*.

Next, using cameras of 360o and fingerprint recognition device. The special cameras of 360o and fingerprint recognition device will be incorporated for identifying the identity. The camera and the fingerprint device will be placed at one location at the place of examination. The 3600 camera is used for the dual purpose of identifying and controlling of examination hall activities. Thus, it utilizes the same resource for identifying the students.

Biometric system, which includes eye-tracking and fingerprint software, has brought a solution to the examination fraud problem. It helps schools to detect unauthorized entry, fake ID cards and others. Fingerprints are used because of their uniqueness. So, the possibility for students to cheat is low. It usually used to authenticate the student's identity before the exam. Same goes to eye tracking, a technology that calculates the eye gaze point as the students look around. Despite using this anti-cheating software technology, students still trying to cheat by putting their notes outside the camera’s view. Their desire to cheat seems impossible to stop even with using this technology. Besides, the student also can ask others help by hiding their friends in the room and asking them to read the answer.

The implementation of biometrics can overcome the traditional way of checking the ID cards of the students during the examination. Biometrics can be used to identify the student as the students enter the exam hall. The IP address can be used to check all this such as using an online signature or displaying student photo and using fingerprint. However, the use of extra devices seems costly to the student, lecturer and universities. Basically, it can provide more security to identify the students by using online cameras which are more useful than the traditional method of checking the ID cards.

Another way to prevent online cheating by using biometric with no extra cost is by using keystroke recognition devices. It can provide school officials with a way to certify the identity of students taking online exams. This keystroke monitoring software technology recognizes and identifies keystroke pattern instead of relying on fingerprint scan or password. In addition, it can also accurately identify the students in the tests as typing characteristics are believed to be unique to the individual and hard to duplicate. The computer will measure the rhythm and speed of the student's typing by doing the typing exercise. Later, the school officials can monitor the typing to see if the pattern match up or not. This program also demonstrates their capability to identify and to authenticate the students via their typing patterns and rhythms with a “high degree of accuracy” through monitoring and to capture unique keyboard events to each individual. It is important to verify the student's identity in online examination environments as the student's enrollment of online classes is increasing, which can build security concern and academic integrity.

2.3 Security

In today's world, the use of applications, and system together with the existence of vulnerabilities, threats, faults, failure and error is inevitable. Hence, the information technology application, devices and models will never be secured. Security is a process of protecting software, hardware and networks against harm (Schechter, 2004). The security goals are commonly referred to as confidentiality, integrity and availability (CIA). Confidentiality used to ensure that assets are restricted to authorized users only. While integrity is to ensure that assets are only altered by authorized users and availability ensures that the system is available and operational. A compromise in the CIA security goals may compromise secure assets.

The security risks have only become more complicated in recent years with the explosion of cloud and mobile technologies (Matthews, 2012). Security dependability and trust need a mechanism for the shifting and should be able to fight upcoming unpredictable threats. A threat is a potential for misuse or abuse that will cause harm or abuse assets. In this research, harm implies a loss of desired system properties such as confidentiality, integrity and availability. The application of security has a broader scope, as well as hardware, software and network security. The focus of this research is application level, which focusing on information security context as described in the next section.

2.3.1 Information Security

The concept of information security is formed from the recognition that “information” is valuable and that it requires protection. As mentioned in the previous section, security is the protection of assets against unauthorized access. In the online learning context, course content, assessment and examination are identified as valuable assets. Any breach of the security goals may cause impairment to the learning process.

The security of online learning faces two challenges which are identity management and authentication. For example, a student is required to prove that “he is who he claims to be”. It is difficult to verify whether or not an assignment was completed and submitted by a valid student or whether some form of cheating takes place (Adetoba B. T., 2016). Identity management and authentication are closely related and embedded in many approaches. The authentication goal is to verify the claimed identity of a user. It has a central role in prevention against identification attacks. Therefore, security in an online learning environment should be given more attention to avoid this threat and to ensure a safer learning environment (Adetoba B. T., 2016) especially for online assessment as described in the next section.

2.3.2 Security in Online Assessment

An assessment is a major element in online learning is especially in a situation where it involves large groups of students. The use of online assessment generally, and online tests in particular, has increased in higher education over the last two decades (Boitshwarelo *et al.*, 2017). High-quality assessments are supposedly dependable, with a high level of reliability and validity. The online assessment is very important to ascertain students' progress (Adetoba B. T., 2016). There are ten broadly types of assessment on online learning which are homework assignments, online tests and/or quizzes, bulletin-board postings, projects or papers, participation in the chat room, proctored tests and or quizzes, team projects, reflective journal, student portfolio and other (Bailie & Jortberg, 2009). However, online examinations are considered an important source for university exam (Sarrayrih & Ilyas, 2013).

Besides, the previous section discussed there is cheating reported when taking online quizzes and exams. The cheating occurs by taking, giving, and receiving forbidden material or information and by circumventing the process of assessment. There is an incentive to cheat both to enter a better university and also to secure a higher grade (Rigby *et al.*, 2015). It is a serious problem affecting educational institutions, and therefore needs urgent attention (Bayaa Martin Saana, Ablordeppey, Mensah, & Karikari, 2016). Therefore, improving the security of online learning will improve the security of online assessments, and this should not be mistreated.

Security is a vital aspect of the online learning system. The goal of security for online learning is to maintain the confidentiality of data or information, the integrity of information and the availability of online learning resources at a certain level while keeping their usability adequate for learners. Authentication is an addition to the three primary security goals, and it has been broadly researched area and seen as the main challenge for online assessment which described in the next section.

2.4 User Authentication

User authentication is a process of verifying a user's legitimate right before secure resources can be released (Kang & Cho, 2015). There are four types of authentication methods, namely, Knowledge Based Authentication (KBA), Object Based Authentication (OBA), Biometric Based Authentication (BBA) and Profile Based Authentication, as shown in Figure 2.2.

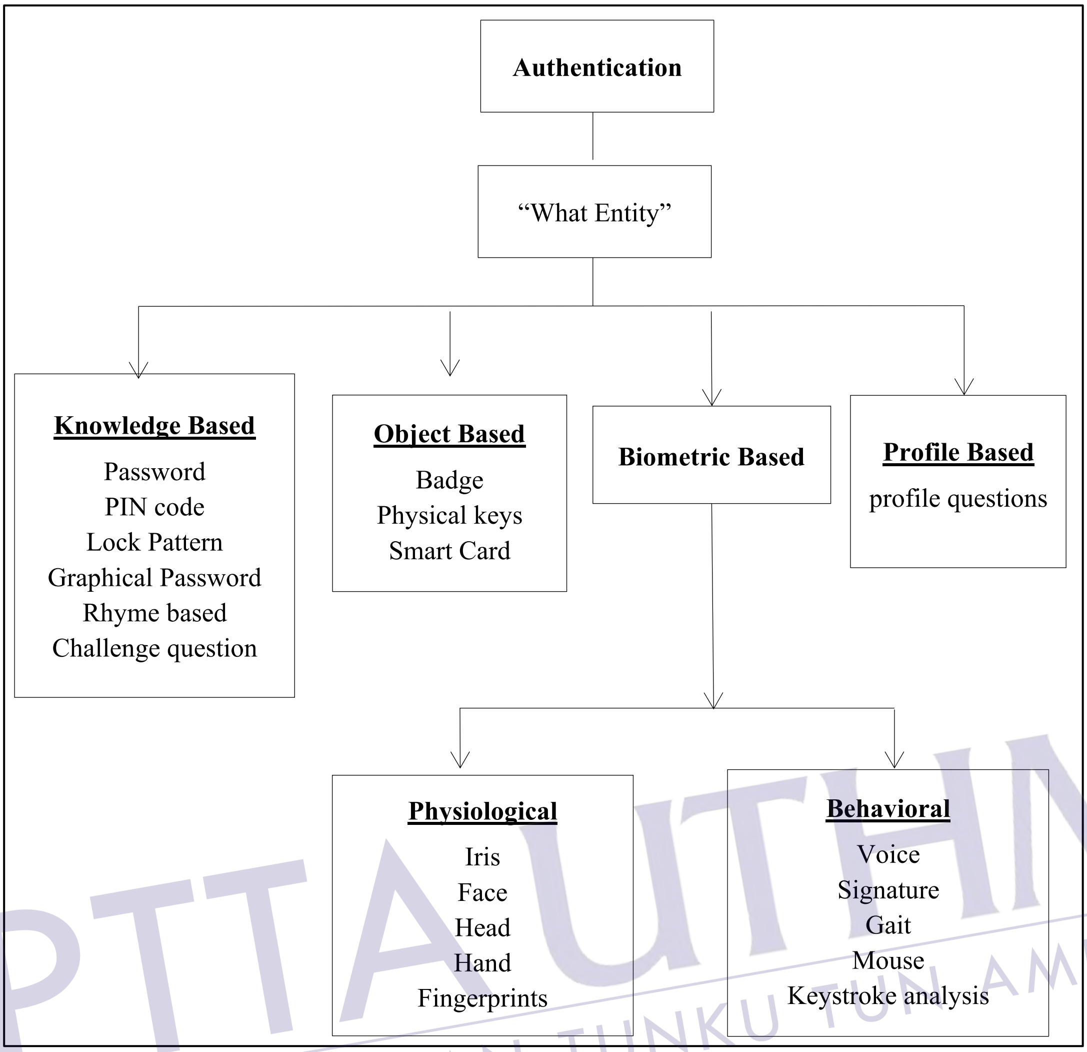

Figure 2.2: Types of Authentication

2.4.1 Knowledge Based Authentication

Knowledge Based Authentication (KBA) is the current predominant authentication method used for online services because it is memorable and it does not require any extra device (Han, Yu, Li, Chen, & Li, 2017). The examples of this method are username, password, and challenge questions that require personal knowledge to authenticate individual access to the online environment. It may include a single word, personal identification numbers (PINs) and phrases which are very closely kept secrets used for creating passwords. However, there is much vulnerability of password, for example, it is exposed to being searched or guessed by an attacker. Besides, the long and random, or changing password is difficult to remember. Thus, it does not provide a good compromise detection, and defense against repudiation (Agashe & Nimbhorkar, 2015).

2.4.2 Object Based Authentication

Generally, an individual in possession of identity objects is believed to be a genuine user to the system. Accordingly, users' identification is done by presenting or applying physical objects, such as magnetic cards, electronic chip cards and digital keys (Ullah et al., 2012). These objects store or generate multiple passwords and provide compromise detection since their absence is observable. They also provide added protection against denial of service attacks (Agashe & Nimbhorkar, 2015). However, there are two main disadvantages of this authentication; it is inconvenient to carry along and it can be costly as it can be easily lost or stolen (Jain, Ross, & Pankanti, 2006). Besides, special-purpose devices also may be required to take record input for registration and authentication (Agashe & Nimbhorkar, 2015).

2.4.3 Profile Based Authentication

In a Profile Based Authentication (PBA) system, a user profile is stored at the verifier and later used to verify their authentication claim by generating challenge questions randomly(Sadikan, Ramli, & Fudzee, 2019). A profile includes user specific information that is privacy sensitive where this information can pertain to personal information, education, activities, professional experience, hobbies, future objectives, and learning activities (Ullah et al., 2012). This authentication used in addition to username and password technique, which used to support student authentication.

It is based on multi-modal authentication which consists of two layers of authentication such as username and password, and challenge questions. Initially, a username and password can be used to login into the online learning environment to carry out regular learning activities during the first layer. While during the learning process, students are posed with profile questions that are used to extend and refine individual student's profile. The second layer of authentication will trigger the challenge questions, which are generated from the student's profile. The profile questions are used to collect answers in order to build and update the student's profile.

REFERENCES

Abdul Razak, Abdul Qayyum. “Analysis of Factors Influencing the Cheating Tendency of Undergraduate UiTM Melaka.” 14 Feb. 2019.

Abisado, M. B., Gerardo, B. D., & Fajardo, A. C. (2017). Towards Keystroke Analysis using Neural Network for Multi - Factor Authentication of Learner Recognition in On - Line Examination. *Manila International Conference on “Trends in Engineering and Technology,”* 71–74.

Abramson, M., & Aha, D. W. (2013). User Authentication From Web Browsing Behavior. *FLAIRS 2013 - Proceedings of the 26th International Florida Artificial Intelligence Research Society Conference*, 268–273.

Adetoba B. T., A. O. and K. S. O. (2016). E-learning Security Issues and Challenges : A Review. *Journal of Scientific Research and Studies*, *3*(5), 96–100.

Agashe, N. M., & Nimbhorkar, S. (2015). A Survey Paper on Continuous Authentication by Multimodal Biometric. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *4*(11), 4247–4253.

Aguiar, R. A., & Sales, R. M. (2010). *Overreact Analysis in the American Stock Market : A Fuzzy C-means Algorithm Approach*. *1*(4).

Al-Asadi, T. A., & Obaid, A. J. (2016). Discovering Similar User Navigation Behavior in Web Log Data. *International Journal of Applied Engineering Research*, *11*(16), 8797–8805.

Aleix, D. J., Morán Moreno, J. A., & Pérez, E. S. (2017). Using Keystroke Dynamics and Context Features To Assess Authorship in Online Learning Environments. *11th International Technology, Education and Development Conference (INTED2017)*, 3167–3176. https://doi.org/10.21125/inted.2017.0819

Alessio, H. M., Malay, N., Maurer, K., Bailer, A. J., & Rubin, B. (2018). Interaction of Proctoring and Student Major on Online Test Performance. *The International Review of Research in Open and Distributed Learning*, *19*(5), 166–185. https://doi.org/10.19173/irrodl.v19i5.3698

Ali, M. L., Monaco, J. V., Tappert, C. C., & Qiu, M. (2017). Keystroke Biometric Systems for User Authentication. *Journal of Signal Processing Systems*, *86*(2–3), 175–190. https://doi.org/10.1007/s11265-016-1114-9

Allen, L. K., Mills, C., Jacovina, M. E., Crossley, S., D'Mello, S., & McNamara, D. S. (2016). Investigating Boredom and Engagement During Writing Using Multiple Sources of Information. *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge - LAK '16*, 114–123. https://doi.org/10.1145/2883851.2883939

Aneja, D., & Rawat, T. K. (2013). Fuzzy Clustering Algorithms for Effective Medical Image Segmentation. *International Journal of Intelligent Systems and Applications*, *5*(11), 55–61. https://doi.org/10.5815/ijisa.2013.11.06

Arkorful, V., & Abaidoo, N. (2014). The Role of E-Learning, The Advantages and Disadvantages of Its Adoption in Higher Education. *International Journal of Education and Research*, *2*(12), 397–410.

Atoum, Y., Chen, L., Liu, A. X., Hsu, S. D. H., & Liu, X. (2017). Automated Online Exam Proctoring. *IEEE Transactions on Multimedia*, *19*(7), 1609–1624. https://doi.org/10.1109/TMM.2017.2656064

Babic, A., Xiong, H., Yao, D., & Iftode, L. (2009). Building Robust Authentication Systems with Activity-Based Personal Questions. *SafeConfig '09: Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration*, 19–24. https://doi.org/10.1145/1655062.1655067

Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User Identification and Authentication using Multi-modal Behavioral Biometrics. *Computers and Security*, *43*, 77–89. https://doi.org/10.1016/j.cose.2014.03.005

Bayaa Martin Saana, S. B., Ablordeppey, E., Mensah, N. J., & Karikari, T. K. (2016). Academic Dishonesty in Higher Education: Students' perceptions and Involvement in an African Institution. *BMC Research Notes*, *9*(1), 1–13. https://doi.org/10.1186/s13104-016-2044-0

Beaudin, S., Levy, Y., Parrish, J., & Danet, T. (2016). An Empirical Study of Authentication Methods to Secure e-learning System Activities Against Impersonation Fraud. *Online Journal of Applied Knowledge Management*, *4*(1), 42–61. Retrieved from http://www.iiakm.org/ojakm/articles/2016/volume4_1/OJAKM_Volume4_1pp42-61.pdf

Behera, T. K., & Panigrahi, S. (2015). Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network. *2nd International Conference on Advances in Computing and Communication Engineering*, 494–499. https://doi.org/10.1109/ICACCE.2015.33

Bemmel, M. B. (2014). Cheating in online classes: A preliminary investigation. Retrieved from https://nsuworks.nova.edu/fse_etd/37/

Bezdek, J. C. (1981). *Pattern Recognition with Fuzzy Objective Function Algorithms*. https://doi.org/10.1007/978-1-4757-0450-1

Bharat, V. M., Atmaram, M. P., & Nirgude, V. N. (2015). Efficient User Navigation Pattern Prediction Technique. *International Journal of Advance Research and Innovative Ideas in Education*, *1*(14), 424–427.

Bhatti, D. M. S., Saeed, N., & Nam, H. (2016). Fuzzy C-means Clustering and Energy Efficient Cluster Head Selection for Cooperative Sensor Network. *Sensors (Switzerland)*, *16*(9), 1–17. https://doi.org/10.3390/s16091459

Bhuvaneswari, M. S., Muneeswaran, K., & Sakthi Priya, K. S. (2018). Fuzzy Clustering of Augmented Web User Sessions. *International Journal of Pure and Applied Mathematics*, *118*(20), 1153–1161. Retrieved from http://www.ijpam.eu

Bixler, R., & D'Mello, S. (2013). Detecting Boredom and Engagement During Writing With Keystroke Analysis, Task Appraisals, and Stable Traits. *Proceedings of the 2013 International Conference on Intelligent User Interfaces - IUI '13*, 225–234. https://doi.org/10.1016/0378-4363(86)90118-X

Boitshwarelo, B., Reedy, A. K., & Billany, T. (2017). Envisioning The Use of Online Tests in Assessing Twenty-first Century Learning : A Literature Review. *Reaserach and Practice in Technology Enhanced Learning*, *12*(16), 1–16. https://doi.org/10.1186/s41039-017-0055-7

Boob, M. A. N., & Dakhane, P. D. M. (2012). Mining Usage Profiles Using Fuzzy Clustering and Its Applications. *International Journal of Emerging Technologies and Advanced Engineering*, *2*(2), 120–123.

Botchkarev, A. (2018). Evaluating Performance of Regression Machine Learning Models Using Multiple Error Metrics in Azure Machine Learning Studio. *SSRN Electronic Journal*, 1–16. https://doi.org/10.2139/ssrn.3177507

Botchkarev, A. (2019). A new typology design of performance metrics to measure errors in machine learning regression algorithms. *Interdisciplinary Journal of Information, Knowledge, and Management*, *14*(January), 45–76. https://doi.org/10.28945/4184

Casey, K. (2017). Using Keystroke Analytics to Improve Pass–Fail Classifiers. *Journal of Learning Analytics*, *4*(2), 189–211. Retrieved from http://dx.doi.org/10.18608/jla.2017.42.14

Castellano, G., Mesto, F., & Minunno, M. (2007). Applications of Fuzzy Sets Theory. In F. Masulli, S. Mitra, & G. Pasi (Eds.), *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-540-73400-0

Chourasia, N. (2014). Authentication of the User By Keystroke Dynamics for Banking Transaction System. *Proceedings of International Conference on Advances in Engineering & Technology*, 41–45.

Clarke, R., & Lancaster, T. (2013). Commercial Aspects of Contract Cheating. *Proceedings of the 18th ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE '13*, 219–224. https://doi.org/10.1145/2462476.2462497

Dahiya, M. (2016). User Authentication Mechanism Based on Neural Networks. *International Journal of COmputer Science and Mobile Computing*, *5*(5), 563–566.

Dandapat, S. K., Pradhan, S., Mitra, B., Choudhury, R. R., & Ganguly, N. (2015a). ActivPass: Your Daily Activity is Your Password. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 2325–2334. https://doi.org/10.1145/2702123.2702457

Dandapat, S. K., Pradhan, S., Mitra, B., Choudhury, R. R., & Ganguly, N. (2015b). ActivPass: Your Daily Activity is Your Password. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 2325–2334. https://doi.org/10.1145/2702123.2702457

Deutschmann, I., Nordstrom, P., & Nilsson, L. (2013). Continuous Authentication Using Behavioral Biometrics. *IT Professional*, *15*(4), 12–15. https://doi.org/10.1109/MITP.2013.50

Dibya, J. B., & Gupta, A. K. (2014). A Comparative Study Between Fuzzy Clustering Algorithm and Hard Clustering Algorithm. *International Journal of Computer Trends and Technology*, *10*(2), 108–113. https://doi.org/10.14445/22312803/IJCTT-V10P119

Diego, L. A. B. (2017). Friends with Benefits: Causes and Effects of Learners' Cheating Practices During Examination. *IAFOR Journal of Education*, *5*(2), 121–138. https://doi.org/10.22492/ije.5.2.06

Dixit, D., & Gadge, J. (2010). A New Approach for Clustering of Navigation Patterns of Online Users. *International Journal of Engineering Science and Technology*, *2*(6), 1670–1676.

Doe, R., Castillo, M. S., & Musyoka, M. M. (2017). Assessing Online Readiness of Students. *Online Journal of Distance Learning Administration*, *20*(1), 1–13. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1140361&site=ehost-live%0Ahttp://www.westga.edu/~distance/ojdla/spring201/doe_castillo_musyoka201.html

Dunn, J. C. (1973). A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters. *An International Journal of Cybernetics and Systems*, *3*(3), 32–57. https://doi.org/10.1080/01969727308546046

Epignosis. (2014). E-Learning Concepts, Trends, Applications. In *Epignosis LLC*. Retrieved from https://www.talentlms.com/elearning/elearning-101-jan2014-v1.1.pdf%0Ahttp://www.talentlms.com/elearning/elearning-101-jan2014-v1.1.pdf

Epp, C., Lippold, M., & Mandryk, R. L. (2011). Identifying Emotional States Using Keystroke Dynamics. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11*, 715–724. https://doi.org/10.1145/1978942.1979046

Fedynich, L., Bradley, K. S., & Bradley, J. (2015). Graduate Students' Perceptions of Online Learning. *Research in Higher Education Journal*, *27*(27), 1–13.

Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2017). Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Systems Journal*, *11*(2), 513–521. https://doi.org/10.1109/JSYST.2015.2472579

G, R. J. (2015). A Review on Fuzzy C-Mean Clustering Algorithm. *International Journal of Modern Trends in Engineering and Research*, *2*(2), 751–754.

Gervais, A., Shokri, R., Singla, A., Capkun, S., & Lenders, V. (2014). Quantifying Web-Search Privacy. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 966–977.

Gilbert, B. (2015). Online Learning Revealing the Benefits and Challenges (Vol. 4).

Giot, R., El-Abed, M., & Rosenberger, C. (2009). GREYC Keystroke: A Benchmark for Keystroke Dynamics Biometric Systems. *IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems, BTAS 2009*. https://doi.org/10.1109/BTAS.2009.5339051

Giot, R., El-Abed, M., & Rosenberger, C. (2012). Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis. *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 11–15. Retrieved from http://arxiv.org/abs/1207.0784

Gomi, H., Tsubouchi, K., Yamaguchi, S., & Sasaya, N. (2017). Towards Authentication Using Multi-modal Online Activities. *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 37–40. https://doi.org/10.1145/3123024.3123097

Habeeb, A. (2017). Artificial intelligence Ahmed Habeeb University of Mansoura. *Research Gate*, *7*(2).

Hameed, M. R., & Abdullatif, F. A. (2017). Online Examination System. *International Advanced Research Journal in Science, Engineering and Technology*, *4*(3), 106–110. https://doi.org/10.17148/IARJSET.2017.4321

Han, G., Yu, Y., Li, X., Chen, K., & Li, H. (2017). Characterizing The Semantics of Passwords: The role of Pinyin for Chinese Netizens. *Computer Standards & Interfaces*, *54*, 20–28. https://doi.org/10.1016/j.csi.2016.10.006

Harun, N., Woo, W. L., & Dlay, S. S. (2010). Performance of Keystroke Biometrics Authentication System Using Artificial Neural Network (ANN) and Distance Classifier Method. *International Conference on Computer and Communication Engineering (ICCCE)*, (May), 1–6. https://doi.org/10.1109/ICCCE.2010.5556852

Hayes, B., & Ringwood, J. V. (2008). Student Authentication for Oral Assessment in Distance Learning Programs. *IEEE Transactions on Learning Technologies*, *1*(3), 165–175. https://doi.org/10.1109/TLT.2009.2

J, J., & Sankaran, S. (2017). A Neuro-Fuzzy Approach for Domestic Water Usage Prediction. *2017 IEEE Region 10 Symposium (TENSYMP)*. https://doi.org/10.1109/TENCONSpring.2017.8070087

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A Tool For Information Security. *IEEE Transactions on Information Forensics and Security*, *1*(2), 125–143. https://doi.org/10.1109/TIFS.2006.873653

Jalali, M., Mustapha, N., Mamat, A., & Sulaiman, M. N. (2008). A New Clustering Approach Based on Graph Partitioning for Navigation Patterns Mining. *International Conference on Pattern Recognition*, *4*(11), 1–4. https://doi.org/10.1109/ICPR.2008.4761808

Just, M., & Aspinall, D. (2009). Personal Choice and Challenge Questions: A Security and Usability Assessment. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS ’09*, 1. https://doi.org/10.1145/1572532.1572543

Kang, P., & Cho, S. (2015). Keystroke dynamics-based user authentication using long and free text strings from various input devices. *Information Sciences*, *308*, 72–93. https://doi.org/10.1016/j.ins.2014.08.070

Karim, N. A., & Shukur, Z. (2015). Review of User Authentication Methods in Online Examination. *Asian Journal of Information Technology*, *14*(5), 166–175. https://doi.org/10.3923/ajit.2015.166-175

Karnan, M., Akila, M., & Kalamani, A. (2009). Feature subset selection in keystroke dynamics using ant colony optimization. *Journal of Engineering and Technology Research*, *1*(5), 72–80. Retrieved from http:/JETR

Khoshnevisan, B., Rafiee, S., Omid, M., Mousazadeh, H., Shamshirband, S., & Hamid, S. H. A. (2015a). Developing a fuzzy clustering model for better energy use in farm management systems. *Renewable and Sustainable Energy Reviews*, *48*(147), 27–34. https://doi.org/10.1016/j.rser.2015.03.029

Khoshnevisan, B., Rafiee, S., Omid, M., Mousazadeh, H., Shamshirband, S., & Hamid, S. H. A. (2015b). Developing a Fuzzy Clustering Model for Better Energy use in Farm Management Systems. *Renewable and Sustainable Energy Reviews*, *48*, 27–34. https://doi.org/10.1016/j.rser.2015.03.029

Killourhy, K., & Maxion, R. (2010). Why Did My Detector Do That?! Predicting Keystroke-Dynamics Error Rates. *Lecture Notes in Computer Science, Vol 6307. Springer, Berlin, Heidelberg*, pp. 256–276. https://doi.org/https://doi.org.ezaccess.library.uitm.edu.my/10.1007/978-3-642-15512-3_14

Killourhy, K. S., & Maxion, R. A. (2012). Free vs. Transcribed Text for Keystroke-Dynamics Evaluations. *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results*, 1–8. https://doi.org/10.1145/2379616.2379617

Kumar, R., & Sharma, M. K. (2016). Advanced Neuro-Fuzzy Approach for Social Media Mining Methods using Cloud. *International Journal of Computer Applications*, *137*(10), 56–58. https://doi.org/10.5120/ijca2016908927

Lakheyan, C., & Kaur, U. (2013). A Survey on Web Usage Mining with Fuzzy c-Means Clustering Algorithm. *International Journal of Computer Science and Mobile Computing*, *2*(4), 160–163.

Lee, P. M., Tsui, W. H., & Hsiao, T. C. (2014). The Influence of Emotion on Keyboard Typing: An Experimental Study Using Auditory Stimuli. *BioMedical Engineering OnLine*, *3*(1), 81–92. https://doi.org/10.1371/journal.pone.0129056

Li, J., & Lewis, H. W. (2016). Fuzzy Clustering Algorithms — Review of the Applications. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 282–288. https://doi.org/10.1109/SmartCloud.2016.14

Liraki, Z., Harounabadi, A., & Mirabedini, J. (2015). Predicting the Users’ Navigation Patterns in Web, using Weighted Association Rules and Users’ Navigation Information. *International Journal of Computer Applications*, *110*(12), 975–8887.

Liu, H., & Kešelj, V. (2006). Combined Mining of Web Server Logs and Web Contents for Classifying User Navigation Patterns and Predicting Users' Future Requests. *Data and Knowledge Engineering*, *61*(2), 304–330. https://doi.org/10.1016/j.datak.2006.06.001

Loschiavo, C. (2017). Why do students cheat? Listen to this dean' s words. Retrieved from The Conversation website: https://theconversation.com/why-do-students-cheat-listen-to-this-deans-words-40295

Loschiavo, F. M., & Shatz, M. A. (2011). The Impact of an Honor Code on Cheating in Online Courses. *Journal of Online Learning and Teaching*, *7*(2), 179–184.

Madara, D. S. (2016). Faculty Perceptions on Cheating in Exams in Undergraduate Engineering. *Journal of Education and Practice*, *7*(30), 70–86.

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2018). Statistical and Machine Learning forecasting methods: Concerns and ways forward. *PloS One*, *13*(3), e0194889. https://doi.org/10.1371/journal.pone.0194889

Mat Zain, Nurul Hidayah. "*Analysis of Factors Influencing the Cheating Tendency of Undergraduate UiTM Melaka*." 4 Feb. 2019.

Matthews, T. (2012). Passwords Are Not Enough. *Computer Fraud and Security*, *2012*(5), 18–20. https://doi.org/10.1016/S1361-3723(12)70044-1

Matyas, V., & Riha, Z. (2002). Biometric Authentication — Security and Usability. *Advanced Communications And Multimedia Security*, *100*(5), 1–13. https://doi.org/10.1007/978-0-387-35612-9_17

Md Shukor, Nur Shahira. "*Analysis of Factors Influencing the Cheating Tendency of Undergraduate UiTM Melaka.*" 31 Jan. 2019.

Melaka, U. T. M. C. (2020). *Laporan Ketersediaan Pensyarah Bagi Pembelajaran & Pengajaran Dalam Talian*.

Michael, T., & Williams, M. (2013). Student Equity: Discouraging Cheating in Online Courses. *Administrative Issues Journal Education Practice and Research*, *3*(2). https://doi.org/10.5929/2013.3.2.8

Midzic, A., Avdagic, Z., & Omanovic, S. (2016). Intrusion Detection System Modeling Based on Neural Networks and Fuzzy Logic. *2016 IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES)*, 189–194. https://doi.org/10.1109/INES.2016.7555118

Mondal, S., & Bours, P. (2017). A Study on Continuous Authentication Using a Combination of Keystroke and Mouse Biometrics. *Neurocomputing*, *230*, 1–22. https://doi.org/10.1016/j.neucom.2016.11.031

Moten, J., Fitterer, A., Brazier, E., Leonard, J., & Brown, A. (2013). Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-Learning*, *11*(2), 139–146.

Muchai, J. (2014). *An Investigation into Factors that Contribute to Cheating in Examinations in Technical Institutions in Central Province, Kenya*.

Nagoriya, V., Yadave, S., Kumar, R., & M, P. L. (2020). iSafe - Authorization using Typing Rhythm : A Survey. *Journal of Emerging Technologies and Innovatives Research (JETIR)*, *7*(4), 46–49.

New, D. (2015). Cheating in Online Classes Is Now Big Business. Retrieved May 3, 2020, from https://www.theatlantic.com/education/archive/2015/11/cheating-through-online-courses/413770/

Nguyen, T. (2015). The Effectiveness of Online Learning: Beyond No Significant Difference and Future Horizons. *MERLOT Journal of Online Learning and Teaching*, *11*(2), 309–319.

Odondo, N. J. (2014). Survey Report on Methods and Reasons Why Students Cheat (A Case Study of Faculty of Science, Egerton University).

Owenga, J. T. O., Raburu, P. A., & Aloka, P. J. O. (2018). Relationship between Selected School Determinants and Examination Cheating tendencies among Kenyan Secondary School Students. *Mediterranean Journal of Social Sciences*, *9*(3), 243–252. https://doi.org/10.2478/mjss-2018-0066

Ozden, M. Y., Erturk, I., & Sanli, R. (2004). Students' Perceptions of Online Assessment: A Case Study. *Journal of Distance Education*, *19*(2), 77–92. Retrieved from http://www.eric.ed.gov/ERICWebPortal/search/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=EJ807820&ERICExtSearch_SearchType_0=no&accno=EJ807820%5Cnhttp://www.eric.ed.gov/PDFS/EJ807820.pdf

Patil, R. A., & Renke, A. L. (2016). Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. *International Journal of Computer Applications*, *144*(9), 27–33.

Paullet, K., & Douglas, D. M. (2014). Verifying User Identities In Distance Learning Courses : Do We Know Who Is Sitting And Submitting Behind The Screen? *Issues in Information Systems*, *15*(I), 370–379.

Prakash, P. G. O. (2016). Analyzing and Predicting User Behavior Pattern from Weblogs. *International Journal of Applied Engineering Research*, *11*(9), 6278–6283. Retrieved from http://www.ripublication.com

Rabiha, S. G., Hendro, Sasmoko, Noerlina, & Ham, H. (2017). Image processing model based E-Learning for students authentication. *2017 International Conference on Information Management and Technology (ICIMTech)*, 187–191. https://doi.org/10.1109/ICIMTech.2017.8273535

Radulovic, U., & Uys, T. (2019). Academic dishonesty and whistleblowing in a higher education institution: A sociological analysis. *African Journal of Business Ethics*, *13*(2). https://doi.org/10.15249/13-2-218

Ramlan Mustapha, & Nik Asilah Nik Ali. (2017). An Empirical Survey of an Academic Dishonesty At a Major Public Universities in Recent Years: The Malaysian Evidence. *Asian Journal of Educational Research*, *5*(3), 43–49.

Reynolds-Seraphin, K., & Collins, J. (2017). No Need To Study. Retrieved August 25, 2017, from https://www.noneedtostudy.com/myclass/

Rigby, D., Burton, M., Balcombe, K., Bateman, I., & Mulatu, A. (2015). Contract Cheating & The Market in Essays. *Journal of Economic Behavior and Organization*, *111*, 23–37. https://doi.org/10.1016/j.jebo.2014.12.019

Rodrigues, M., Gonçalves, S., Carneiro, D., Novais, P., & Fdez-Riverola, F. (2013). Keystrokes and Clicks: Measuring Stress on E-learning students. *Second International Symposium Management Intelligent Systems*, *220*, 119–126. https://doi.org/10.1007/978-3-319-00569-0_15

Ryan, S., Kaufman, J., Greenhouse, J., She, R., & Shi, J. (2016). The Effectiveness of Blended Online Learning Courses at the Community College Level. *Community College Journal of Research and Practice*, *40*(4), 285–298. https://doi.org/10.1080/10668926.2015.1044584

S.Shraddha. (2014). Intrusion Detection using Artificial Neural Network. *Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence Intrusion*, (1), 209–217.

Sadeghi, M. (2019). Manijeh Sadeghi 1. *International Journal of Reserach in Englissh (IJREE)*, *4*(1), 80–88.

Sadikan, S. F. N., Ramli, A. A., & Fudzee, M. F. M. (2019). A survey paper on keystroke dynamics authentication for current applications. *AIP Conference Proceedings*, *2173*(November), 020010. https://doi.org/10.1063/1.5133925

Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous User Authentication using Multi-modal Biometrics. *Computers and Security*, *53*, 234–246. https://doi.org/10.1016/j.cose.2015.06.001

Sahoo, S., & Ratha, B. K. (2018). Rapid Frequent Pattern Growth and Possibilistic Fuzzy C-means Algorithms for Improving the User Profiling Personalized Web Page Recommendation System. *International Journal of Intelligent Engineering and Systems*, *11*(2), 237–245. https://doi.org/10.22266/ijies2018.0430.26

Saoreen Rahman, Mamun, S. Al, Ahmed, M. U., & Kaiser, M. S. (2016). PRY / MAC Layer Attack Detection System Using Neuro-Fuzzy Algorithm for loT Network. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2531–2536. IEEE.

Sawant, M. M., Nagargoje, Y., Bora, D., Shelke, S., & Borate, V. (2013). Keystroke Dynamics: Review Paper. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(10), 4018–4020. Retrieved from www.ijarcce.com

Shaker, S. H., Saydani, R. J., & Obaid, M. K. (2014a). Keystroke Dynamics Authentication Based on Principal Component Analysis and Neural Network. *International Journal of Scientific and Engineering Research*, *5*(6), 830–837. https://doi.org/ISSN 2229-5518

Shaker, S. H., Saydani, R. J., & Obaid, M. K. (2014b). Keystroke Dynamics Authentication Based on Principal Component Analysis and Neural Network. *International Journal of Scientific and Engineering Research*, *5*(6), 830–837.

Sheila, M., Faizal, M. A., & Shahrin, S. (2014). Learner Centric in M-Learning: Integration of Security, Dependability and Trust. *10th International Conference Mobile Learning 2014*, 318–322.

Sheware, S., & Nikose, A. A. (2015). Web Usage Mining Based on Server Log File Using Fuzzy C-Means Clustering. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *4*(10), 3300–3308.

Shih, Y. E., & Mills, D. (2007). Setting the New Standard with Mobile Computing in Online Learning. *International Review of Research in Open and Distance Learning*, *8*(2), 1–16. Retrieved from http://www.tonybates.ca/2010/08/21/cheating-in-online-learning/

Silambarasan, G., & Shathik, J. A. (2017). Fuzzy Set based Evolving User Prediction and Classification for Recommendation Model. *International Journal of Pure and Applied Mathematics*, *117*(15), 1151–1162. Retrieved from http://www.ijpam.eu

Silviu, B. (2010). Fuzzy Clustering. *Babes-Bolyai University*, 40–61. https://doi.org/10.4018/978-1-5225-0997-4.ch003

Simhachalam B, Ganesan, G. (2015). Fuzzy Clustering Algorithms in Medical Diagnostics. *Kärntner Botanikzentrum*, *22*(7).

Singh, B., Sonawane, S., Shah, Y., & Singh, V. (2017). Literature Survey on Keystroke Dynamics for User Authentication. *International Journal on Recent and Innovation Trends in Computing and Communication*, *5*(5), 280–282. Retrieved from http://www.ijritcc.org

Stanciu, V.-D., Spolaor, R., Conti, M., & Giuffrida, C. (2016). On the Effectiveness of Sensor-enhanced Keystroke Dynamics Against Statistical Attacks. *Proceedings of the Sixth ACM on Conference on Data and Application Security and Privacy - CODASPY '16*, 105–112. https://doi.org/10.1145/2857705.2857748

Starovoytova, D. (2016). Factors Affecting Cheating-Behavior at Undergraduate-Engineering. *Journal of Education and Practice*, *7*(31), 66–82.

Stewart, J. C., Monaco, J. V., Cha, S. H., & Tappert, C. C. (2011). An Investigation of Keystroke and Stylometry Traits for Authenticating Online Test Takers. *International Joint Conference on Biometrics*, 1–7. https://doi.org/10.1109/IJCB.2011.6117480

Suganya, R., & Shanthi, R. (2012). Fuzzy C- Means Algorithm- A Review. *International Journal of Scientific and Research Publications*, *2*(11), 1–3.

Sujatha, V., & Punithavalli. (2012). Improved User Navigation Pattern Prediction Technique From Web Log Data. *International Conference on Communication Technology and System Design*, *30*(2011), 92–99. https://doi.org/10.1016/j.proeng.2012.01.838

Sun, Y., Ceker, H., & Upadhyaya, S. (2017). Shared Keystroke Dataset for Continuous Authentication. *International Workshop on Information Forensics and Security*, 0–5. https://doi.org/10.1109/WIFS.2016.7823894

Sundari, M. R., Srinivas, Y., & Reddy, P. P. (2014). A Review on Pattern Discovery Techniques of Web Usage Mining. *International Journal of Engineering Research and Applications*, *4*(9), 131–136. Retrieved from www.ijera.com

Swan, K. (2019). Research on Online Learning. *Research on Online Learning: Students, Faculty, Instituition*, *11*(1), 55–59. https://doi.org/10.24059/olj.v11i1.1736

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, *48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Taher, F., Werghi, N., Al-Ahmad, H., & Sammouda, R. (2012). Lung Cancer Detection by Using Artificial Neural Network and Fuzzy Clustering Methods. *American Journal of Biomedical Engineering*, *2*(3), 136–142. https://doi.org/10.5923/j.ajbe.20120203.08

Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *The Scientific World Journal*, *2013*. https://doi.org/10.1155/2013/408280

Teh, P. S., Teoh, A. B. J., Yue, S., Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal*, *2013*, *2013*, e408280. https://doi.org/10.1155/2013/408280, 10.1155/2013/408280

Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2015). Recognizing Your Touch: Towards Strengthening Mobile Device Authentication via Touch Dynamics Integration. *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia - MoMM 2015*, 108–116. https://doi.org/10.1145/2837126.2837127

Trivedi, J. A. (2014). Voice Identification System Using Neuro-Fuzzy Approach. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, *2*(3), 300–301. Retrieved from http://www.ijarcst.com/doc/vol2-issue3/ver.2/jeegar.pdf

Ullah, A. (2016). *Security and Usability of Authentication by Challenge Questions in Online Examination*.

Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2012). Using Challenge Questions for Student Authentication in Online Examination. *International Journal of Infomomics*, *5*(3), 631–639.

Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2014). Privacy and usability of image and text based challenge questions authentication in online examination. *2014 International Conference on Education Technologies and Computers (ICETC)*, 24–29. https://doi.org/10.1109/ICETC.2014.6998897

Usman, A. K., & Shah, M. H. (2013). Strengthening E-Banking Security Using Keystroke Dynamics. *Journal of Internet Banking and Commerce*, *18*(3), 1–14. https://doi.org/10.1007/978-3-531-92534-9_12

Valera, J., Valera, J., & Gelogo, Y. (2016). A Review on Facial Recognition for Online Learning Authentication. *Proceedings - 8th International Conference on Bio-Science and Bio-Technology, BSBT 2015*, 16–19. https://doi.org/10.1109/BSBT.2015.15

van Griethuijsen, R. A. L. F., van Eijck, M. W., Haste, H., den Brok, P. J., Skinner, N. C., Mansour, N., … BouJaoude, S. (2015). Global patterns in students' views of science and interest in science. *Research in Science Education*, *45*(4), 581–603. https://doi.org/10.1007/s11165-014-9438-6

Vellingiri, J. (2011). Fuzzy Possibilistic C-Means Algorithm for Clustering on Web Usage Mining to Predict the User Behavior. *European Journal of Scientific Research*, *58*(2), 222–230.

Vellingiri, J., Kaliraj, S., Satheeshkumar, S., & Parthiban, T. (2015). A Novel Approach for User Navigation Pattern Discovery and Analysis for Web Usage Mining. *Journal of Computer Science*, *11*(2), 372–382. https://doi.org/10.3844/jcssp.2015.372.382

Vimalil, J. S., & Taj, Z. S. (2015). FCM based CF: An Efficient Approach for Consolidating Big Data Applications. *IEEE International Conference on Innovation, Information in Computing Technologies (ICIICT 2015)*, 1–7. https://doi.org/10.1109/ICIICT.2015.7396090

Vinayak, R., & Arora, K. (2015). A Survey of User Authentication using Keystroke Dynamics. *International Journal of Scientific Research Engineering & Technology (IJSRET)*, *4*(4), 378–384. Retrieved from https://doi.org/10.1371/journal.pone.0129056

Vinayakvitthal, L., & Charniya, N. N. (2015). Review of Advances in Neural Network Based Biometric Authentication. *IEEE International Conference on Communications and Signal Processing (ICCSP)*, 735–740. https://doi.org/10.1109/ICCSP.2015.7322587

Vural, E., Huang, J., Hou, D., & Schuckers, S. (2014). Shared Research Dataset to Support Development of Keystroke Authentication. *International Joint Conference on Biometrics*. https://doi.org/10.1109/BTAS.2014.6996259

Wang, G., Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems with Applications*, *37*(9), 6225–6232. https://doi.org/10.1016/j.eswa.2010.02.102

Wankhede, S. B., & Verma, S. (2014). Keystroke Dynamics Authentication System Using Neural Network. *International Journal of Innovative Research and Development*, *3*(1), 157–164. Retrieved from http://www.ijird.com/index.php/ijird/article/view/46133%5Cnhttp://www.ijird.com/index.php/ijird/article/download/46133/37479

Wu, Y., Duan, H., & Du, S. (2015). Multiple fuzzy c-means clustering algorithm in medical diagnosis. *Technology and Health Care*, *23*(s2), S519–S527. https://doi.org/10.3233/THC-150989

Xu, J., & Lambert, J. H. (2015). Risk-Cost-Benefit Analysis for Transportation Corridors with Interval Uncertainties of Heterogeneous Data. *Risk Analysis*, *35*(4), 624–641. https://doi.org/10.1111/risa.12231

Yao, F., Yerima, S. Y., Kang, B., & Sezer, S. (2017). Continuous Implicit Authentication for Mobile Devices based on Adaptive Neuro-Fuzzy Inference System. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2017)*. https://doi.org/arXiv:1705.06715

Younis, M. I., & Hussein, M. S. (2015). Construction of an Online Examination System with Resumption and Construction of an Online Examination System with Resumption and Randomization Capabilities. *International Journal of Computing Academic Research (IJCAR)*, *4*(2), 62–82.

Zhang, Y., Wang, J., Han, D., Wu, H., & Zhou, R. (2017). Fuzzy-Logic Based Distributed Energy-Efficient Clustering Algorithm for Wireless Sensor Networks. *Sensors*, *17*(7), 1554. https://doi.org/10.3390/s17071554

Zhong, Y., Deng, Y., & Jain, A. K. (2012). Keystroke Dynamics for User Authentication. *Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference*, 117–123. https://doi.org/10.1109/CVPRW.2012.6239225

Zulfadhilah, M., Prayudi, Y., & Riadi, I. (2016). Cyber Profiling Using Log Analysis and K-Means Clustering: A Case Study Higher Education in Indonesia. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *7*(7), 430–435. https://doi.org/10.14569/IJACSA.2016.070759