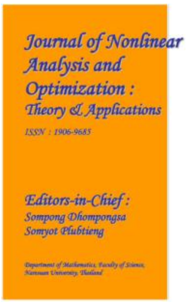
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**



Journal of Nonlinear
Analysis and
Optimization :
Theory & Applications
ISSN : 1906-9685

Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

Department of Mathematics, Faculty of Science,
Naresuan University, Thailand

ANALYSIS INSUFFICIENT STUDENT COMMUNICATION IN ONLINE TEST ENVIRONMENT USING ELECTRONIC MONITORING SYSTEM

[1]M. GOPI SAI   [2]Dr. RATNA RAJU MUKIRI

[1]M.Tech Scholar, Dept. of CSE, St. Ann's College of Engineering & Technology, Chirala

[2]Associate Professor, Dept of CSE, St. Ann's College of Engineering & Technology, Chirala

Email: m.gopisai@gmail.com

Abstract: Now a day's online exam has become one of the prominent and most important aspects of our lives, but there is no guaranty of genuinity of the result in the online examination processes**.** Mostly the challenge of security for sensitive data also arises when they are outsourced by users to cloud. a technique to detect cheating in MCQ tests is proposed in a proposed adaptive elearning system, where web usage mining techniques and the k_means algorithm with Levenshtein distance are used to detect cheating by dividing the learners into clusters according to the similarity in the numbers of their choices in the MCQ test. Distributed data duplication system is used in cloud storage to reduce memory space & upload bandwidth only one copy every file stored in cloud even if that file is used by number of users. The proposed system performs a set of tasks, including detecting the identity of the examinee, the presence and absence of the examinee, the presence of more than one person next to the examinee, attempts to use a cell phone, and tracking the examinee's eye movement. To determine the behavioral metric during online examination the researcher identified, Switching between the examination windows, level of engagement. Typing speed and accuracy, Examining the frequency and duration, Security analysis depicts that our deduplication systems secure in terms of the definitions specified in the proposed security model. The paper also proposes a Fraud Detection based Online Test [FDOT] and Behavior identification through Visualization Techniques [BIVT] that avoids and performs more effectively compared with the existing systems.

Index Terms: Fraud Detection, Behavior identification, malpractice, Data Visualization, Web mining, Web usage mining, E-learning, Adaptive E-Learning, K-Means.

1. INTRODUCTION

In online exams the location of the proctor and examinee are at different locations since the communication is through online using internet [1] it reduces the total data that needs to be physically stored by eliminating extra information and replacing after repetition of it with a pointer to the original. K-means clustering algorithm is an unsupervised algorithm that is used to cluster a group of data objects into a number of clusters [10], each cluster includes a set of objects with similar properties among themselves, and these objects are different from the objects in other clusters [2]. Furthermore for the data security challenge is also arises more sensitive data are redistributed by the users to cloud. Encoding have been usually Utilized, for to provide security confidentiality before the redistributed data into cloud [3]. One of the advantages of e-learning is that it reduces costs, is available to all individuals and different age groups, and is flexible because there are no time-related links [4]. The TPA is nothing but who has expertise and capabilities that users is periodically check the integrity of all the data stored in the cloud on behalf of the users which gives easiest way for the users to give ensured of their storage correctness in the cloud [5]. The traditional methods of curbing cheating in examinations by checking students properly, sitting arrangements and banning digital gadgets in examinations rooms are more commonly used in majority of the traditional face to face examination centers withing the African region [6]. This proposed technique to detect cheating in MCQ tests in a proposed adaptive system, where usage-based web mining techniques are used with its steps data collections, data preprocessing, pattern discovery and pattern analyzes. And the K-means algorithm distance criterion is used in pattern discovery step also created the IQ feature for each learner to help confirm the case of cheating [7].

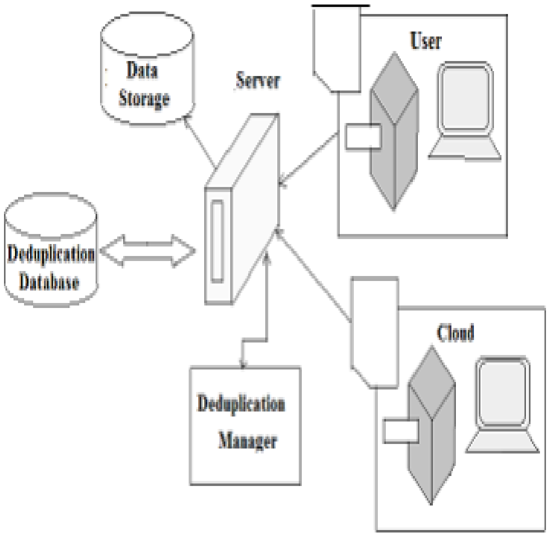


Fig. 1: Data Flow Diagram

2. RELATED WORK

The length of the axis determines the attribute contribution. Table lens technique uses rows and columns for representing the data items and attributes. [8]. The advantage of the proposed work is improving web prediction accuracy. It can be used to prefetch the web pages before they are being requested by the user, this reduces the access latency [9]. In 1997 M. Bellare explained the idea of security and scheme for symmetric encryption. Cloud computing is architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources number of types of networks, storage, servers, services and applications, without physically acquiring [10]. In this paper characteristic points are extracted from the examinee's face and then used to estimate head position. Suspicious behavior is also detected based on differences in yaw angle, presence of sound. [11]. Data sharing is refers to storing data at a place where it can use by multiple users at the same time ensuring the security of data. In this project data is shared using a secured model is use of encryption for ensuring security of data as well as it also contains mechanisms for authentication of users [12]. Recently in the era of pervasive artificial intelligence (AI), an exploration was undertaken to determine integration of AI. The main goal of this research is to improve the functionality of one of the components software agent called Fraud Detector purpose is to track attempts to cheat during exams, made by the students..

3. SYSTEM ARCHITECTURE

Academic fraud can occur in various settings, including online environments. The conceptual framework presented in this text highlights several factors that contribute to academic fraud in online settings. [13]. This technique is used to improve storage uses and applied to network data transfers to reduce the number of bytes that must be sent. Since this data is structured, it’s stored in relational database (currently MySQL [29]). Using external AI, we could leverage from its huge knowledge base and functionalities, adding additional skills to our agent and measuring its performance [14]. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information documents are typically read and how often. We change total search behaviors that exhibit deviations from the user baseline the correlation of search behavior errors detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector’s accuracy [15].

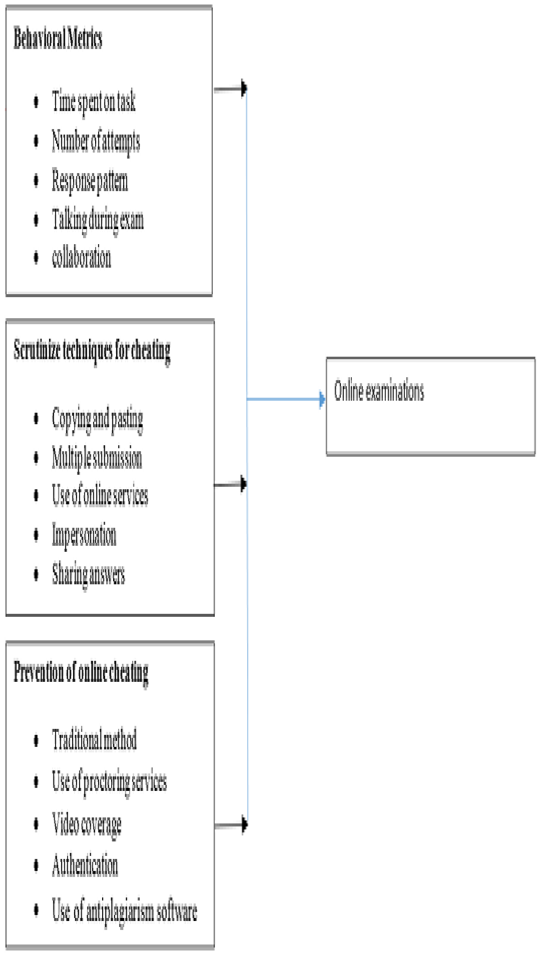


Fig. 2: System Architecture.

4. PROPOSED METHODOLOGY

The detection and comparison of the student's face and behavior is done in two steps. Firstly preprocessing is done to the image through filtering, normalization and segmentation [16]. The proposed system is optimization and general public auditing system of information storage security in cloud computing and user privacy-preservation auditing protocol. The assumption information integrity threats toward users data are that they will come from each internal and external attack at Cloud Server (CS). These can be hardware failures, software bugs, bugs in the network path, economically change hackers, malicious or accidental management errors. In this task, a technique is proposed using web usage mining techniques, where the K-means clustering algorithm is used to cluster the data, represented by the numbers of Learners' choices in the MCQ test, to cluster these data into clusters according to the amount of similarity between the numbers of Learners' choices on the questions. The output of this clustering process is clusters each cluster contains a set of choice number series for the tested questions and each series belongs to each Learner [17].

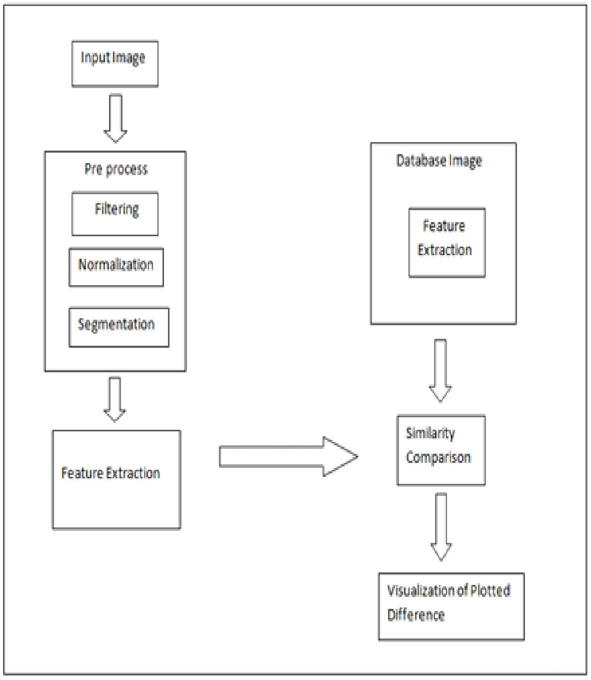


Fig. 3: Fraud Detection based Online Test [FDOT] and Behavior identification through Visualization Techniques [BIVT].

5. PROPOSED ALGORITHM

This proposed technique is to make a recommendation report on cheating in the MCQ test by recommending Learners among whom there is a possibility of cheating the Levenshtein distance is used to compare each of the two series and measure their similarity [18]. The framework provided the guide because we had to look at each category of the interdisciplinary levels to find out what contributions came from each as well as the number of efforts made [19]. The process of identifying the student’s identity is repeated in different periods throughout the exam period. In addition, a number of other requirements must be met for the system to function properly [20].

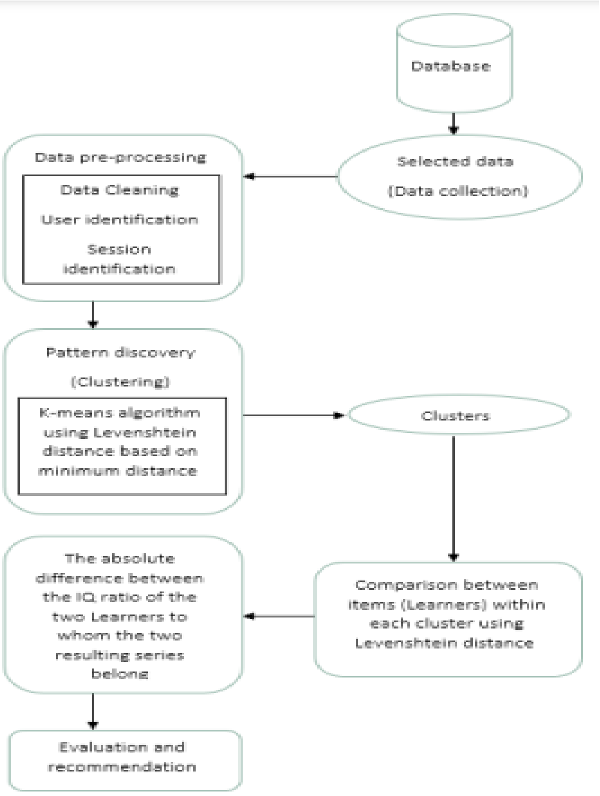

Database
Selected data
(Data collection)
Data pre-processing
Data Cleaning
User identification
Session identification
Pattern discovery
(Clustering)
K-means algorithm using Levenshtein distance based on minimum distance
Clusters
The absolute difference between the IQ ratio of the two Learners to whom the two resulting series belong
Comparison between items (Learners) within each cluster using Levenshtein distance
Evaluation and recommendation

Fig. 4: - Block diagram of report cheating cases in the MCQ test technique task

Step1: Ccollecting of data The first step is to collect the relevant data from the data log file. This data is represented in the proposed system by the Learner's choices numbers on the questions for each MCQ test,

Step2: Data preprocessing In the data preparation step, the data is first cleaned of noise and the empty data records are deleted. Secondly, in the process of preparing the data, users or Learners are identified through the ID of each user or Learner

Step3: **Pattern discovery** In the process of pattern detection, the k-means clustering algorithm is used, and the Levenshtein distance (LD) is used to measure the distance between the center and the elements

Step4: Comparison between Items (Learners) within each cluster using Levenshtein distance After the clustering process is completed, the output is a set of clusters. Each cluster contains a group of convergent Learner choices number series

Step 5: The absolute difference between the IQ ratio of the two Learners to whom the two resulting series belong After the comparison step is completed and the two sequences belonging to two

Learners appear, it is necessary to strengthen the recommendation of this technique to these two Learners as a case of cheating.

6. PROPOSED ELECTRONIC MONITORING SYSTEM

Identity identification of the examining student Python language and libraries like CV2, SKlearn, Face recognition and NumPy with KNN (K nearest classifier) algorithm were used to detect and distinguish the examinee's face as well as detect the presence of more than one person inside the exam room. At system startup, the identity detection software will be executed and this task will be repeated throughout the test period, using a webcam with a resolution. The software extracts a frame from the camera's video and begins to recognize faces in that frame by comparing it to the set of images in the previously prepared database [19]. A cluster based K-nearest-neighbors-classified face recognition system and bootstrap assembly were used KNN is derived and based on the Near Classifier (NN) system. This classifier is based on a simple non-parametric decision. The distance between the features of each query image and the features of the other images in the training data set is analyzed [20].

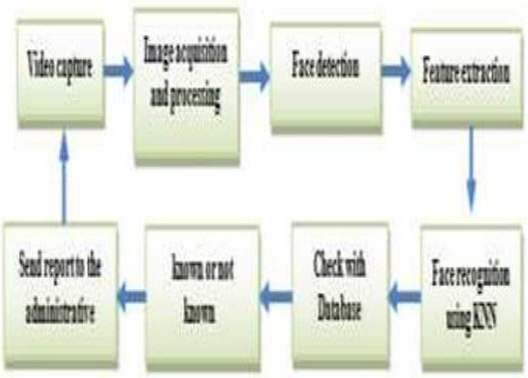

Video capture
Image acquisition and processing
Face detection
Feature extraction
Face recognition using KNN
Check with Database
known or not known
Send report to the administrative

Fig. 5: Steps for student identification

Pupils Tracking Media Pipe Iris is a machine learning algorithm for iris estimation that tracks iris landmarks, pupil and eye contours in real time using the camera and without specialized hardware. It can determine the metric distance between object and camera with less than (10%) error. We needed to understand; first, about deep learning techniques; second, how can we use this deep learning technique to detect cheat during online exams.

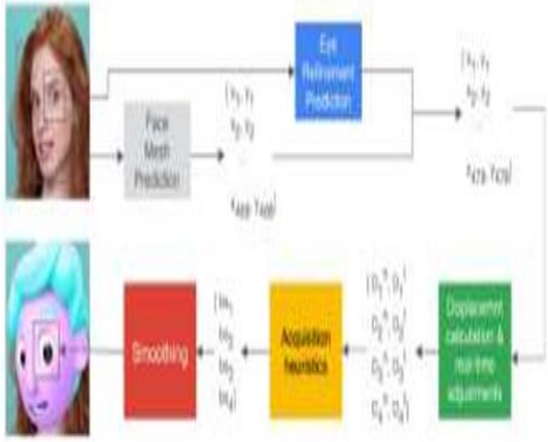

Eye Refinement Prediction
Face Mesh Prediction
Smoothing
Acquisition heuristics
Displacement calculation & real-time adjustments

Fig. 6: Overview of the pupil blend shapes acquisition

7. RESULT ANALYSIS

The proposed data is the initial proposed Learner data to test the proposed technique, which has been proposed in a variety of ways to test the validity of the technique's work. Fifty-four Learner accounts are created. The tests of applying the system on the webcam images of the cases studied in this research showed that the accuracy varies according to the type of the object, and this is due to the number of features that can be detected by the object, as well as to the type of algorithms used in the detection and resolution of the webcam used in our system. A lot of research has been done regarding the same. A number of solutions have been seen, however implementation of some of the models are prohibitively expensive. Few researchers in IT have tried the same but somehow used some of the science lab techniques in conjunction with AI, especially Machine Learning algorithms such Naïve Bayes, kNearest Neighbor and so on.

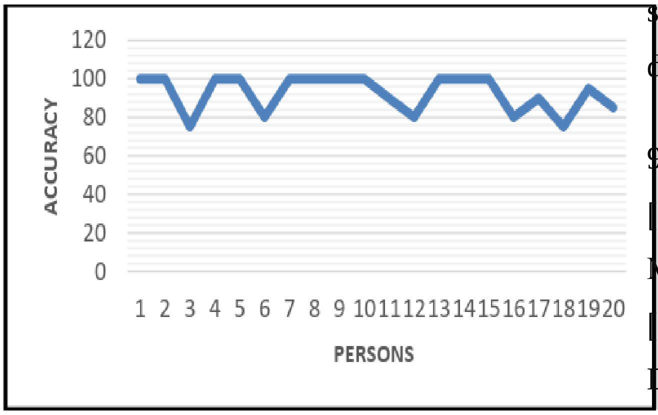


Fig. 7: Pupil track accuracy

8. CONCLUSION

We proposed set of authentication techniques are discussed. They include passwords, tokens, and biometrics. Special conditions are involved, to make the techniques to be strong enough to the intruder attacks. It is worth noting that in the clustering process using the k-means algorithm for the cheating detection technique, the problem of the algorithm not stopping appeared, as this problem is solved by determining the number of iterations in the algorithm. A set of requirements have been set for the system to function properly, including providing good lighting, as well as not allowing the student to make some movements, which are considered an attempt to cheat. Security through username and password user is select the file and default mode of upload. This project would be designed to perform better than other file sharing tools available. The results obtained indicate that the proposed system was effective in supervising the exam and contributed significantly to reducing cheating attempts during the electronic exam.

9. .REFERENCES

[1] Christopher Mallow," Authentication Methods and Techniques"

[2] Kim Bartke, 2005" 2D, 3D and High-Dimensional Data and Information

Visualization", Seminar on Data and Information Management

[3] Winnie Wing-Yi Chan, 2006; "A survey on Multivariate Data Visualization", Department of Computer Science and Engineering. Hong Kong University of Science and Technology

[4] Ryszard S.Choras, 2007,"Image Feature Extraction Techniques and their Applications for CBIR and Biometric System", International Journal of Biology and Biomedical Engineering

[5] Andrzej Materka and Michal Strzelecki, 1998 "Texture Analysis Methods – A Review", Technical University of Lodz, Institute of Electronics ul. Stefanowskiego

[6] U. C. Apoki, H. K. M. Al-Chalabi, and G. C. Crisan, "From Digital Learning Resources to Adaptive Learning Objects: An Overview," Communications in Computer and Information Science, vol. 1126 CCIS. pp. 18–32, 2020. doi: 10.1007/978-3-030-39237-6_2.

[7] R. D. Ara´ujo, R. G. Cattelan, and F. A. Dorc¸a, "Towards an Adaptive and Ubiquitous Learning Architecture," 2017 IEEE 17th International Conference on Advanced Learning Technologies Towards. pp. 539– 541, 2017. doi: 10.1109/ICALT.2017.63.

[8] P. Chopade, S. M. Khan, D. Edwards, and A. Von Davier, "Machine Learning for Efficient Assessment and Prediction of Human Performance in Collaborative Learning Environments," 2018 IEEE International Symposium on Technologies for Homeland Security, HST 2018. 2018. doi: 10.1109/THS.2018.8574203

[9] openCV team, "about openCV", https://opencv.org/about/.

[10] Natali Almeida, "Facial Recognition System applied to Multipurpose Assistance robot for Social Human-robot Interaction (MASHI)", M.S. thesis, Escuela Técnica Superior de Ingeniería Industrial de Barcelona, Barcelona, 2017.

[11] Adam Geitgey, "face recognition",https://face-recognition.readthedocs.io/en/latest/readme.html. GitHub, Inc.