How to Cite:
Gnanabaskaran, A., Kumar, S. S., & Nishanth, A. S. (2022). Biometric based online student identity verification and proctoring. *International Journal of Health Sciences, 6*(S5), 5702–5714. https://doi.org/10.53730/ijhs.v6nS5.9888

Biometric based online student identity verification and proctoring

Dr. A. Gnanabaskaran
Assistant professor in Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India.
Email: gnanabaskarana@ksrct.ac.in

S. Sunil Kumar
Students of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India
Email: sunilvj006@gmail.com

A. Shri Nishanth
Students of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India
Email: shrinishanth247@gmail.com

***Abstract*---**Students who write exams online and proctored using biometrics methodology today. Especially for online certification, training organizations need to check that the students who completed the learning process and received the academic credits are those who registered for the courses. Moreover, they have to ensure that these students complete all the online training activities without cheating or inappropriate behaviors. The COVID-19 pandemic has accelerated (abruptly in certain cases) the migration and implementation of online education strategies and consequently the need for safe mechanisms to authenticate and monitor online students. There are several technologies with different grades of automation in these days. This project deeply describes a specific solution based on the authentication of different biometric technologies and an automatic proctoring system, which incorporates features to solve the main concerns in the market: highly scalable, affordable, automatic, with few software requirements for the user, reliable and passive for the student. Finally, the technological performance test of the large scale system, the usability privacy perception survey of the user and their results are discussed in this project. The project contains admin module in which student personal details with finger print and photo during enroll. During verification, student needs to give photo and fingerprint so that verification process succeed. During proctoring, the

screen capturing is taken place at regular intervals and is being sent to admin system for monitoring. The project contains node addition, process to be listened or all processes, time between taking screen shots and upload schedule. During node addition, the node id, IP address, system name are added. In addition, process list for selected users are added and if the users runs the process, then it is highlighted in admin user. Moreover, the administrator user is able send alert message to selected user. The project is designed using Microsoft Visual Studio .Net 2019 as front end with C# coding and MS SQL SERVER 2010 as back end. Likewise, the process started and stopped log are also viewed by administrator. The mail is sent to administrator if a wanted process is accessed by the node user. This helps the administrator to monitor the nodes from any place efficiently.

***Keywords*---**Biometric, online student, COVID-19, proctoring system.

I. Introduction

Nowadays, there are commercial solutions in the market as well as research publications that try to solve this problem. Some of them only authenticate the identity, others monitor, some in real time, others record the sessions. Some cover only exams or specific activities. Some are totally human based solutions (non-scalable) or fully automatic ones (non-reliable). There are also a few scientific approaches which develop the idea of combining some of the cited functionalities. There seems to be, however, no comprehensive and dependable solution that combines multi-biometric continuous authentication with continuous visual and audio monitoring, device activity monitoring and lock-down options, and human supervision (only when necessary) to assure 100% reliable outcomes. We describe a revolutionary approach in this research that gives commercial solutions to all of the problems identified. Based on web applications, it offers continuous biometric (face, fingerprint image) recognition for identity service to online students (biometric traits cannot be lost, stolen, or recreated), as well as automatic continuous proctoring through automatic image and audio processing (device monitoring, lock-down, and inappropriate behaviour detection), allowing online courses to become more valuable for both organisations and students.

This system is based on highly accurate digital signal processing and biometric recognition algorithms, and it is supplemented with human oversight in cases where the automatic algorithms are unable to produce trustworthy results. It can be used to continually authenticate the students at any time during the course of the learning process, not just at particularly delicate points.It is contact-less and needs only a low level of user collaboration. In addition, the whole system is based on cloud computing technologies, which removes geographical and technological barriers for online learning providers.

There is no doubt that online learning has been gaining popularity throughout the past years. This phenomenon is not surprising given that online learning allows education institutes to operate at a lower cost and with greater reach out to more

students. Educational institutions are offering courses online to leverage the benefits of online learning. This is especially so since the advent of Massive Open Online Courses (MOOC). On the other hand, COVID-19 has been a challenge for traditional institutes offering face-to-face teaching, and these institutions have had to migrate (in a very short period of time) to a fully online education model The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas. forced by the pandemic situation. However, online learning implementation presents challenges. E-learning has a serious deficiency, which is the lack of efficient mechanisms that assure user authentication, in the system login as well as throughout the session. Especially for online certification and accreditation, the training organizations need to verify that the online learners who completed the learning process and received the academic credits are precisely those who registered for the courses. Inadequate methods of identity verification affect the reliability of credentials and certification earned online.

The ability to authenticate and monitor online users is becoming more important due to the increase of the internet world (e-learning, e-banking, e-gambling, e-government). Since first human based online proctoring systems, various fully or semi-automatic authentication and proctoring technologies based on biometric features have appeared in the last few years. Bio-metrics has proved itself to be one of the best methods for recognizing people based upon physiological or behavioural characteristics [3]. These technologies can be divided into two categories: those that are based on physical characteristics and those that are based on behaviour characteristics. The former includes face recognition, fingerprint scanners, iris scanners, vein matching, etc. The latter includes voice recognition, handwriting recognition, keystroke dynamics, etc. It is proved that no technology will provide the right answer on its own, but that the combination of different solutions will come up with the appropriate functionality depending on customer needs. Furthermore, the majority of remote authentication proctoring methods require some amount of human involvement for fully trustworthy service, which restricts scale.

II. Literature Review

[1] Keystroke dynamics is a behavioural biometric trait that can be used to identify people based on how they type. Keystroke dynamics are a nearly universal method for subject authentication on the Internet, despite the fact that keystroke biometrics have a high intra-class variability for person recognition, especially in free-text scenarios (i.e., the input text typed is not changed between enrollment and testing).The global keystroke bio-metrics market is projected to grow from $129.8million dollars (2017 estimate) to $754.9millionby 2025, a rate of up to 25% per year1. As an example, Google has recently committed $7 million dollars to fundTypingDNA2, a startup company which authenticates people based on their typing behavior.

The measurement of keystroke dynamics depends on the acquisition of key press and release events. This can occur on almost any commodity device that supports text entry, including desktop and laptop computers, mobile and touch screen devices that implement soft (virtual) keyboards, and PIN entry devices such as

those used to process credit card transactions. Generally, each keystroke (the action of pressing and releasing a single key) results in a key down event followed by key up event, and the sequence of these timings is used to characterize an individual's keystroke dynamics. Within a web browser, the acquisition of key down and key up event timings requires no special permissions, enabling the deployment of keystroke biometric systems across the Internet in a transparent manner.

[2] Any cyber security programme should include user authentication as a key component. However, only validating a user's identity once is not sufficient to offer dependable security for the duration of the user session. To make sure that only authorised users are using the system resources throughout the entire session, continuous session monitoring is required in this regard. This work proposes and implements a real continuous user authentication system with keystroke dynamics behavioural biometric modality.A novel method of authenticating the user on each action has been presented which decides the legitimacy of current user based on the confidence in the genuineness of each action. The two-phase system, which includes ensemble learning and a robust recurrent confidence model (RRCM), leverages a novel perception of two thresholds, namely the alert and final thresholds. The proposed methodology classifies each action using an ensemble classifier's probability score, which is then combined with R-RCM hyper parameters to compute the current confidence in the user's genuineness. Based on the updated confidence value and final threshold, the system determines whether or not the user can continue to use the system. When the alert threshold is reached, however, it tends to lock off imposter users more rapidly. Furthermore, the system was validated using two separate experimental settings, with findings provided in terms of mean average number of genuine actions (ANGA) and average number of impostor activities (ANIA), with experimental setting II obtaining the lowest mean ANIA. A robust continuous user authentication (CUA) system should meet two basic requirements. Firstly, it should not disturb the user while it is performing any tasks on system and work passively by gathering the behavioural information of users. Secondly, CUA should authenticate the user continuously on every single activity that user is performing. In order to meet these requirements, one possible way is to use behavioural bio-metrics e.g., keystroke dynamics which may play an important role to validate the user's identity throughout the session by distinguishing one user from another. Moreover, most of behavioural bio-metrics i.e., the keystroke dynamics do not require users to present biometric identification while preforming important routine tasks and also tends to authenticate the user on each single key press action. Keystroke dynamics recognition (KDR) can be referred as a behavioural bio-metrics which comprises of evaluating the computer user's distinct typing patterns followed by recognition of person's identity based on these patterns. In terms of implementation, there are numerous advantages for the usage of KD as a recognition method [5] since these are practical and inexpensive where no additional hardware component is required in order to capture the KD bio-metrics as oppose to other bio-metrics which require special hardware like fingerprints, iris and facial bio-metrics. Keystroke dynamics can add an additional security layer that continuously verifies the user's identification throughout the session, but they cannot replace the conventional initial login procedures. Due to the incomplete data and significant intra-class differences in

the data acquired by the computer input devices, analysing user behaviour for continuous authentication is a difficult process. As a result, the majority of earlier research used an analysis based on a fixed number of actions or fixed time period, known as episodic authentication. In this method, the system records the keystroke timings for a fixed number of actions or fixed block size before analysing the data to determine whether it comes from a real user or not. On the other hand, a genuine continuous authentication system tends to confirm the user's identity after each keystroke [6]. The keystroke timing information used by the KD-based authentication system is acquired by the keyboard with the aid of specially created software [7], and several discrete attributes are derived from those timestamps.

This section presents the speculative basis and preceding research works leading to the proposed system. The majority of earlier studies in the field of keystroke dynamics typically concentrated on static user authentication (SUA), whereas relatively little work has been done on continuous user authentication (CUA). However, as more people rely on computers and mobile devices for daily chores including office work, online shopping, online banking, and more, CUA is becoming increasingly common due to security concerns of systems and applications. The team of researchers did preliminary study on CUA utilising keyboard dynamics in 1995 [8], and some noteworthy findings were published.

User templates are created by calculating the mean and standard deviation of each key hold time and key digraph flight and latency [12]. On the other hand, some research studies [6] had featured the mean and standard deviation of only those digraphs which had occurred least number of times in order to build the inimitable feature set. Moreover, the researchers in [13] had employed the combination of key digraph, trigraph, error corrections and word per minute features to build the user profiles. In other research [14], the feature set had also been expanded to include digraphs, trigraphs, and a few more related n-graphs. While other researchers extracted the characteristics set using certain terms that are frequently found in English, such as the, an, and, to, etc. [15]. Moreover, in [16] researchers had combined the timing features with non-timing features i.e., pressure, position, finger placement and finger choice for tying behaviour analysis. It has been observed that most of the research work had built statistical user profiles based on mean and standard deviation of specific keys and key-pairs. However, this type of approach is better suited for fixed text, on the contrary, for the free text where user must be using some key-pairs which are missing from statistical profile can lead to low accuracy. In contrast, this research work has considered the approach of taking keystroke dynamics data as sequential series and analyzing the user behavior serially instead of measuring on statistical profile.

The programming language used throughout this work is Python 3.4. Keas interface with tensor flow is employed to execute the neural network computations precisely. Scikitlearn is used to train the SVM. Here, we present some excerpts of our results based on 512 action sequence where the user has been authenticated on each action. However, in practice validation has been done on whole of validation split data (20%) and aggregated results are provided in

tabular form but here for sake of understanding only some samples of results are shown in order to visualize the user categories.

[3] The popularity and reach of massive open online courses (MOOCs) and other kinds of distance education continues to grow. The ability to successfully proctor remote online tests is a key limiting issue in this next stage of education's scalability. Human proctoring is currently the most frequent method of assessment, which involves either forcing test takers to visit an examination centre or monitoring them visually and audibly throughout exams via a webcam. However, such approaches are time-consuming and expensive. We describe a multimedia analytics system that does automatic online exam proctoring in this research. he system hardware includes a webcam, a wearcam, and a microphone for monitoring the visual and audio environment of the testing location. The six main components that constantly examine the important behaviour indications are user verification, text detection, voice detection, active window detection, gaze estimation, and phone detection. By combining the continuous estimating components and adding a temporal sliding window, we can classify whether the test taker is cheating at any time during the exam. We collect multimodal (audio and visual) data from 24 participants who engaged in various sorts of cheating while taking online exams to evaluate our suggested solution. Extensive testing results show that our online exam proctoring technology is accurate, reliable, and efficient. For online students, the standard testing technique is to go to an on-campus or university-certified testing centre and take an exam while being proctored by a human. Students can take examinations anywhere they have an Internet connection thanks to new emerging technologies like Kryterion and ProctorU. They do, however, still rely on someone to "monitor" the exam taking. Kryterion, for example, uses a human proctor who monitors a test taker via camera from a remote location. The proctor is trained to look for and listen for any strange test taker actions, such as peculiar eye movements or moving out of the field of view. He has the ability to warn the test taker or even stop the test. We present a multimedia analytics system for doing automatic and continuous online exam proctoring (OEP) in this study. The general purpose of this system is to ensure exam academic integrity by offering real-time proctoring in order to catch the bulk of test taker cheating actions.

The current digital era unavoidably demands an extensive application and exchange of digital documents. Almost all companies and organizations, regardless of size and scope, have to make use of certain systems for storing a huge amount of data. It is easier to store and search data compared to conventional techniques in which data were being stored with use of numerous files, then to find required data, users had to search for them in a lot of files. This strategy causes data security to become a key issue.

Thus, biometric systems have get popular in terms of data protection from any probable risk [11]. Biometrics systems verify and identify individuals through the use of their biometric traits like behavioral characteristics.

[4]Data collection and storage in a large size is done on a routine basis in any company or organization. To this end, wireless network infrastructure and cloud computing are two widely-used tools. With the use of such services, less time is

needed to attain the required output, and also managing the jobs will be simpler for users. In order to store data in a digital database, general services use a unique identification. It might, however, come with some restrictions and difficulties. The data holder's name, address, identity card number, etc., are linked to the unique identification. Attackers have the ability to modify a unique identifier to steal the entire data set. Attackers might even eavesdrop or guess to obtain the necessary data.It results in lack of data privacy protection. As a result, it is necessary to take into consideration the data privacy issues in any data digital data storage. With the use of current services, there is a high possibility of exposure and leak of data/information to an unauthorized party during their transfer process. In addition, attacks against services, such as spoofing attacks, forgery attacks, and so on, may occur during information transactions. This research proposes using a biometric authentication method based on a palm vein during the authentication procedure to mitigate such dangers. Furthermore, to make the database record anonymous, a pseudonym creation approach is used, ensuring that the data is adequately protected.This way, any unauthorized party cannot gain access to data/information. The proposed system can resolve the information leaked, the user true identity is never revealed to other In current world, all companies and organizations have to hold a huge amount of digital data in storage. The database systems utilized for such purposes need to be properly standardized and well structured in such a way that managing and preserving the data can be done simply. The applied program needs to satisfy the requirements of clients like information holding, personal management, and national statistics, authorization of data tracking, and assistance in administration. In addition, the system used for data preservation must be capable of enhancing the efficiency level of the database record services. c. Thus, information is linked simply; any central authority does not exert any form of control or limitation on the information flow. Their system helps to control the information and to share data in a privacy-friendly exchange environment. According to their reports, their proposed system has been verified in the universal compos ability (UC) framework. They also gave reliable examples on the basis of discreet-logarithm-related assertion.

The current digital era unavoidably demands an extensive application and exchange of digital documents. Almost all companies and organizations, regardless of size and scope, have to make use of certain systems for storing a huge amount of data. It is easier to store and search data compared to conventional techniques in which data were being stored with use of numerous files, then to find required data, users had to search for them in a lot of files. This strategy causes data security to become a key issue. Thus, biometric systems have get popular in terms of data protection from any probable risk [11]. Biometrics systems verify and identify individuals through the use of their biometric traits like behavioral characteristics (e.g., signature and handwriting) or physiological features (e.g., palmprint, fingerprint, palm vein, voice, iris). According to [12], verification process validates that the individual is who she/he claims to be. This process is done through making a comparison between the individual’s trait and the biometric profile corresponding to that individual, which exists in database (i.e., one-to-one search). On the other hand, identification actually searches the unknown identities or unknown biometric through making

a comparison between the existing biometric characteristic and lots of other features that exist within the database (i.e., one-to-many search).

As an alternative to palmprint and fingerprint (due to their limitations), palm vein, which has some unique features, has been proposed. Reference [15] maintained that palm vein is not simply altered, damaged, or fabricated. As a result, for identity verification purposes, it can be offered with a high security and reliability. In recent years, systems of palm vein recognition have become very popular since the privacy and security issues have become more significant for companies and organizations. This popularity is also because of the fact that nowadays companies and organizations have to store and manage a huge amount of data. In addition, the palm vein recognition is applicable to authentications and privacy protection purposes, for instance, to gain access to an ATM machine, login into a computer system, gain access to healthcare system, etc. The palm vein popularity is also due to the wider and more complex vascular patterns on individuals' palm, which shows a wealth of distinguishing characteristics.

III. Proposed methodology

To avoid the drawbacks in the existing system and reduce the time consumption, a system is required such that if the application is doing monitoring process of all systems and report them to web server database. The new system includes photo image and finger print image input along with username and password during the login process. The proposed system uses systematic listening through watching programmatically in systems by installing the application in all nodes. The administrator need now watch on all systems such that any unwanted process is accessed by users. This increases the efficiency of monitoring especially when the nodes are more in count. The new system reduces the time consumption in verification about processes accessed by users.

The first step in the software development life cycle is the identification of the problem. As the success of the system depends largely on how accurately a problem is identified. At present, building the network monitoring process is potentially one of the biggest tasks of network administrators; it is complex, time consuming, and consume most of time efforts, costs, and resources. So, this project identifies that and helps for efficient monitoring through listening unwanted running processes and taking snap shots and send to administrator. The software used to solve the problem and develop the application is Microsoft Visual Studio.Net with C# as programming language and MS-SQL Server 2008.

Admin

Add Process

In the add process module consist of the process id, process name and along with the process path details, these details are used to store the process details for monitoring the process.

Add Student

In student addition module, register number, name, gender, department, studying year, batch, mobile number, email id and password is given. In addition,

face photo and finger print image is also selected for that student. The details are saved in students table.

Add Question Papers
In question paper addition module, question id, question, answer choice 1 to 4 and correct answer is saved. The details are saved in questions table.

Monitoring the System
In the monitoring system is used to monitor the each and every system for which of the unwanted process is to logged and send the mail to admin, with the information of the logged system name, process name.

View Students
In student view module, register number, name, gender, department, studying year, batch, mobile number, email id are displayed. In addition, face photo and finger print image is also displayed for that student. The details are taken from students table.

View Questions papers
In question papers view module, question id, question, first answer choice, second answer choice, third answer choice and fourth answer choice are displayed along with correct answer. The details are taken from questions table.

View Exam Result
In exam results view module, register number, student name, question id, question, select answer, result (correct or wrong) are displayed along. The details are taken from exams table.

View Process Log
All the process log details can be viewed, searched and updated using a data grid view control.

View Snapshots
All the snapshot details can be viewed, searched and updated using a data grid view control.

View Process details
All the process details can be viewed, searched and updated using a data grid view control.

Students

- Login
- Write Exam
- View Exam Results

Login

In login module, register number, and password along with face photo and finger print image is given as credentials. The condition is checked with students table and then login succeeds.

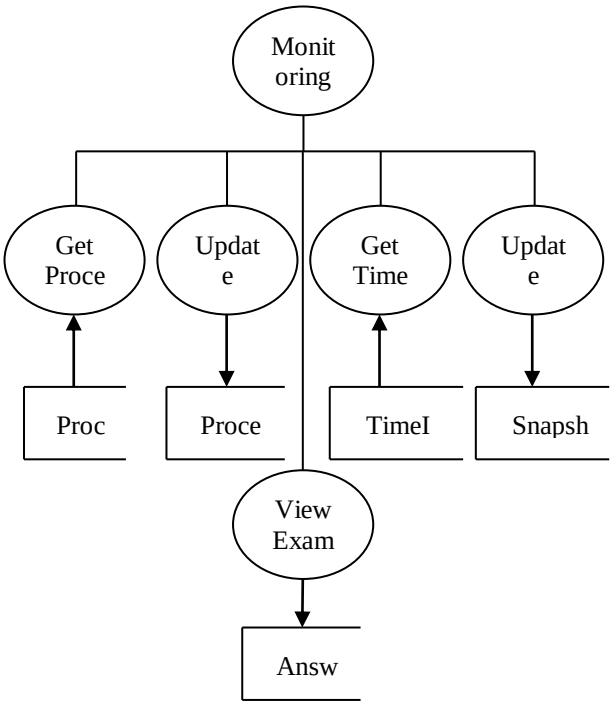
Write Exam

In exam module, question id, question, answer choices are displayed in which questions are generated randomly from questions tables, Then the choice is selected. Mark is calculated immediately based on correct or wrong answer. After all the questions are answered, the total mark is displayed along with all choices selected. The record is saved in exams table.

View Exam Result

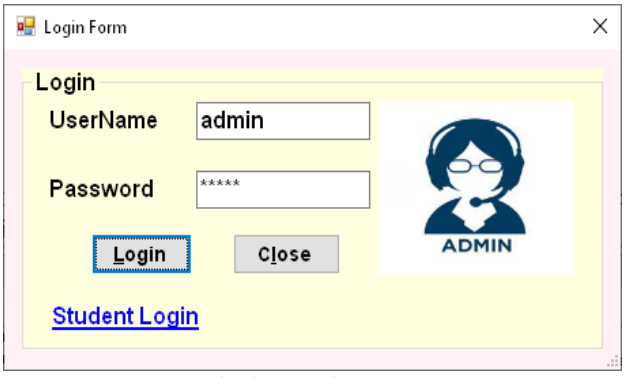
In exam results view module, register number, student name, question id, question, select answer, result (correct or wrong) are displayed along. The details are taken from exams table.

Use Case Diagram

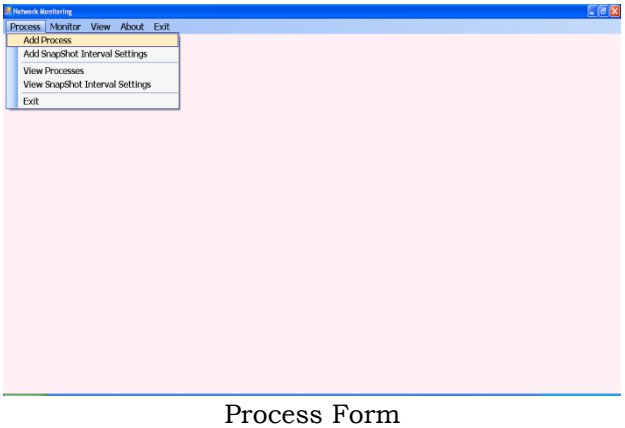


5712

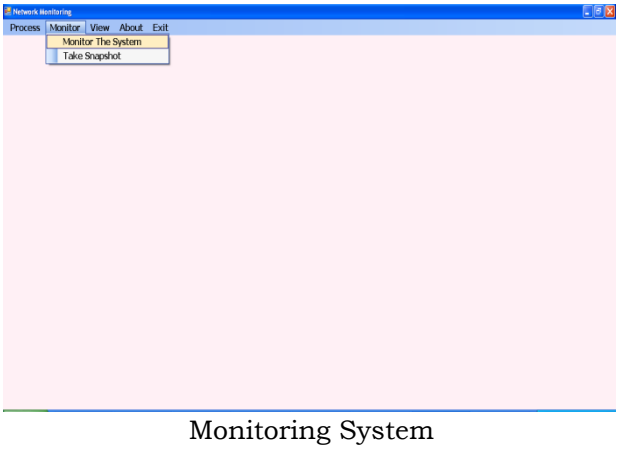
Images



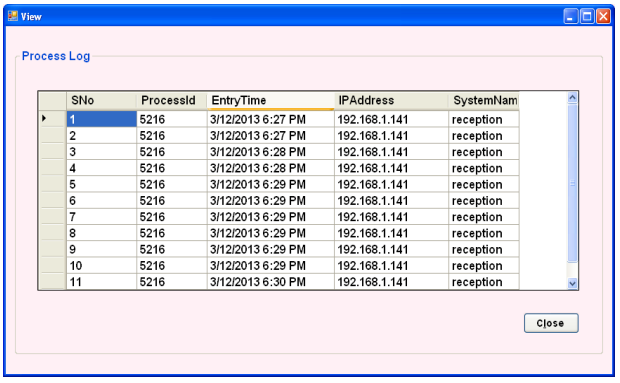
Admin Login Form



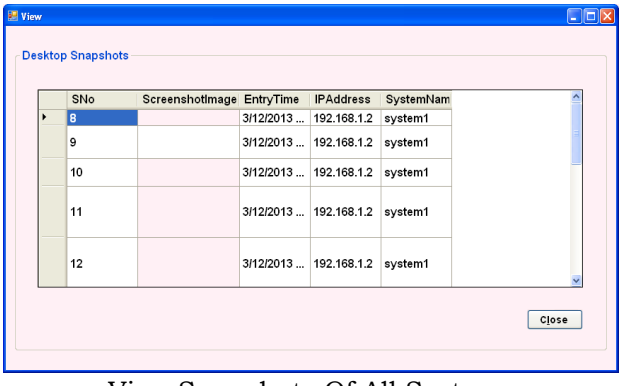
Process Form



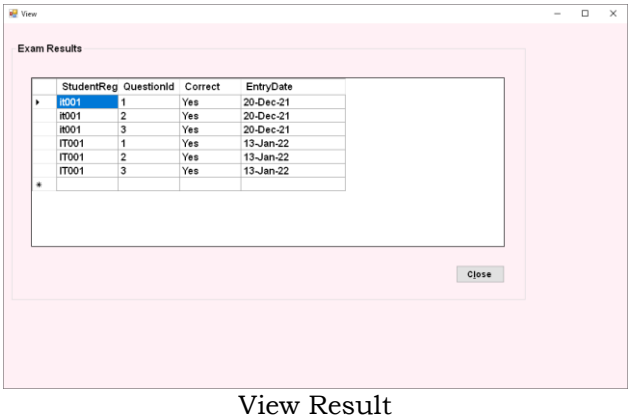
Monitoring System



View Process Log Of All Systems



View Snapshots Of All Systems



View Result

IV. Conclusion

The project is very effective to network administrators. This project is quite simple and easy to understand for the end users. The user's Login feature provides some security features. Only authorized users can access the Information.

This project is very compatible in nature. Further enhancements can be effective to the flow of the project. The main motto behind feature enrichment is to encompass advanced monitoring tool and this factor is considered and implemented to the possible extent.

Thus we may conclude that, this package is found useful as it reduces the time consumption and advanced feature of monitoring even taking snapshots of nodes and update to administrator's web site. The system was provided to be flexible and user friendly. The package may satisfy all kind of user as well as the software professionals.

V. Scope for Future Development

The application developed for different database handling in effective way. There is some scope for further development. At present, all the nodes are treated as equal important and process details are updated to database. In future, different nodes can be set with different processes list so that one process may be allowed in one system but not in other.

References

1. Keystroke Dynamics for User Authentication.Yu Zhong Yunbin Deng Advanced Information and Technology BAE Systems (2020).
2. Continuous User Authentication Featuring Keystroke Dynamics Based on Robust Recurrent Confidence Model and Ensemble Learning Approach (2020).
3. TypeNet: Deep Learning KeyStroke Dynamics.Alejandro Acien, Aythami Morales, John V. Monaco, Ruben Vera-Rodriguez, Julian Fierrez (2021).
4. A Novel Secure Fingerprint-based Authentication System for Student's Examination System (2019).
5. Rinartha, K., & Suryasa, W. (2017). Comparative study for better result on query suggestion of article searching with MySQL pattern matching and Jaccard similarity. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). IEEE.
6. Automated Online Exam Proctoring Yousef Atoum, Liping Chen, Alex X. Liu, Stephen D. H. Hsu, and Xiaoming Liu (2015).
7. Rahman, N. M., Made, S., Usman, A. N., Idris, I., Unde, A., & Bahar, B. (2022). Analysis of understanding of midwife students of midwife care as the impact of online learning. International Journal of Health & Medical Sciences, 5(1), 63-66. https://doi.org/10.21744/ijhms.v5n1.1834
8. Automatic Exam Correction Framework (AECF) for the MCQs, Essays, and Equations Matching Hossam Magdy Balaha And Mahmoud M. Saafan (2021).