International Journal of Pure and Applied Mathematics
Volume 119 No. 15 2018, 1705-1712
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue
http://www.acadpubl.eu/hub/

St. Joseph's Institute of Technology
3rd International Conference on Recent Trends in Engineering and Technology
4th and 5th May 2018

MULTI-FACTOR AUTHENTICATION SCHEME FOR ONLINE EXAMINATION

Naveen Joshy, M Ganesh Kumar, P Mukhilan,V Manoj Prasad, T Ramasamy,Harini N
Student, Student, Student, Student, Student, Asst Professor
Dept of Computer Science and Engineering,Amrita School of Engineering, Coimbatore.Amrita Vishwa Vidyapeetham, India
{CB.EN.U4CSE15521@cb.students.amrita.edu,CB.EN.U4CSE15216@cb.students.amrita.edu, CB.EN.U4CSE15235@cb.students.amrita.edu, CB.EN.U4CSE15232@cb.students.amrita.edu, CB.EN.U4CSE15245@cb.students.amrita.edu, n_harini@cb.amrita.edu}

ABSTRACT

Multi-factor authentication schemes have emerged as alternatives to single-factorauthentication schemes with the aim of improving the security. Factors like passwords, biometrics smart/id cards have been used in combinations in addition to mobile OTPs for enhancing security. Conventional authentication schemes are inadequate for security-criticalapplications like financial transaction, online examinations,etc. The paper focuses on discussing a multi-factor authentication scheme specifically designed for securing online examination services without comprising user-friendliness. The experimentation results clearly brought out the applicability of the scheme in real time with fine-tuningof network related parameters.

Keywords: Authentication, Password, Biometrics, Security, Data Protection, Secure Login Verification

INTRODUCTION

In a world where everything is moving towards digitization, online examinations have become part and parcels of our life. The traditional art of pen and paper examination is slowly becoming obsolete and internet-based exams are gaining popularity, transitioning to accommodate ourselves to the digital era. An online examination refers to the process of a computerized test for the evaluation of a student/candidate in a particular domain. The major advantage that an online examination system provides is the reduction of costs and time for both the candidate and the evaluator. It serves as a measure for the improvement of accuracy for the entire exam management system as a whole.

With this increasing demand for online examination, fraudulence involved in this has also seen an immense rise [12]. Though the total annihilation of cheating seems like an impossible task with all the advanced technology out today, it can be controlled to a large extent. Students resort to several cheating measures starting from copying from their neighbors to the extent of forging the identity by sending other people to undertake the exam on their behalf.

Though it offers a simple platform for conducting and evaluating students, security management has always been a major challenge to the Online Examination System. The security measures for online examinations prevalent follows a hierarchical structure. Some methodologies that are currently deployed include Knowledge-Based authentication using usernames and passwords, and a Webcam-based facial recognition system. But the major drawback that one faces in the current online examination system isthe problem that it is based on a single-factor authentication system which makes it easily vulnerable to the cheating mechanisms. The work presented here aims at overcoming authentication-related problems in online examination systems with a multi-factor based authentication scheme

The paper is organized as follows: Section I gives a general outlook on the Online Exam Management System; Section II gives a glimpse of the related work in this domain; Section III talks presents the proposed multi-factor authentication scheme for enhancing of security of the online examination system; Section IV discusses experimentation results related to the study; And finally Section V presents conclusions with scopefor future extensions.

Abbreviations and Acronyms

CA: Certification Authority, QR: Quick Response.

RELATED WORK

In the system proposed in [1] uses integrated palm print with traditional username password combo to authenticate. Palm print authentication is an emerging biometric feature. The paper insists deployment of webcams to continually supervise the examinee. However, a major drawback to the system is that the continuous surveillance might cause slight uneasiness to the examinee.[2] emphasizes on keystroke pattern combined with traditional username and password to serve the purpose of authentication. It is claimed that cost of implementation of this technique will be considerably low as no special hardware is required. It states that the system provides continuous surveillance without costing examinees privacy. But the drawback of this system is that it has low accuracy and permanence since the user typing pattern changes with familiarity with typing[6].A system using IP address and timestamps to check for malpractices is proposed in [3] for monitoring distance learning exams taken by students. He uses IP address of examinee and timestamps to check for malpractices. No special hardware is required for implementing this technique. Using timestamps and IP address we can check no two students have taken the test together. The problem is that IP addresses, though they are unique, can be easily manipulated using VPNs.A profile-based authentication framework combined with user-id and password for authentication is suggested in [4]. It follows a simple implementation and requires no special hardware. Theefficiency of the system depends upon the challenge questions used and the number of questions used. If the answers to these questions are shared, then there is a chance that examinee might cheat in the exam.Another variation is a scheme based on Yaw angle variation [8]. They use a webcam to capture audio and video. From the video input, feature points are extracted and yaw angle variations are calculated and audio input is compared with a threshold value. Based on this video and audio analysis, whether an examinee has indulged in malpractice or not is determined. This system doesn't require any special hardware. [10] proposes a method for physically challenged people to take the online tests. While all other systems use keyboards, mouse,and other biometric devices, this system uses the voice, which helps the physically challenged people to take the test with ease like others. Since it uses a single factor authentication, it is prone to impersonation.A method using a zip disk containing the required files for the test is proposed [13]. All these files are encrypted and can only be opened by the client program that is been included in the disk. During initialization, the client program also verifies the network card address (MAC address).

The development of the Internet has brought with it widespread online and offline education. The requirements of an Online Examination include accessibility, monitoring ,and management tasks. Related to security the requirements include authentication, integrity, maintenance,copy prevention and detection,cheating prevention,etc.The security requirements are generally provided using symmetric and asymmetric cryptosystems and digital signature schemes [14]. The exam administrator authenticates the examinee using authentication factors registered with a trusted registration authority. Prevention of fraudulent activities is performed using e-monitoring services. This paper is targeted towards exams administered through the Internet and requires exam administrator to monitor and authenticate entities using Face Recognition, Fingerprint ,and OTP tokens.

PROPOSED SYSTEM

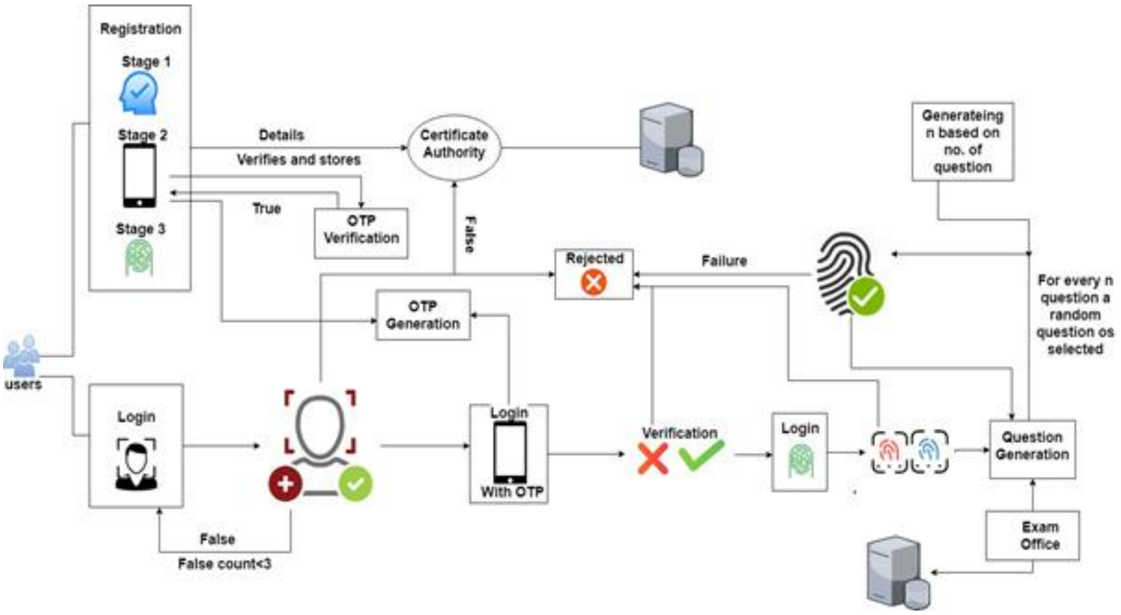
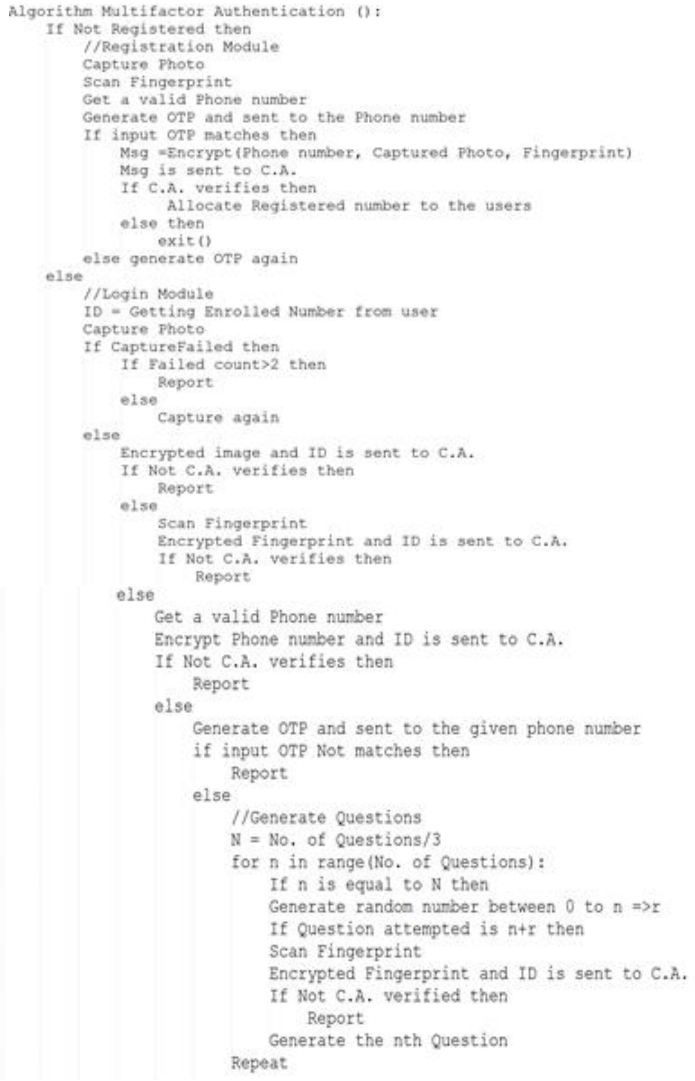


Fig. 1 Architecture Diagram

Unlike the other systems already prevalent which follow a single-factor authentication [9], the proposed system in this paper follows a multi-factor authentication process which features Face-Recognition, OTP verification ,and Fingerprint Authentication modules. The system deploys a hierarchical structural methodology where the user starts off with a proper Registration process. The registration process involves the user registering himself/herself with a unique Register ID provided by the institution, Right Forefinger impression and his/her personalized cellphone number verified using OTP. Once the Registration process is done, the system proceeds to Login module. The Login module provides access for users into the System. It begins with a user being prompted to enter the registration ID after which the webcam captures a photo of the user which undergoes a facial recognition process to test the authenticity of the user. Once failed, an additional chance is being granted to the user. However, on failing twice the user is denied access to the system and a report is sent to the Controlling Authority. Following the Face-recognition module, the user has to bypass an OTP verification process. In this module, an OTP is automatically generated and sent to the registered mobile number. On failing to enter the correct OTP, the user is denied access. Once successfully completing the OTP process, the user is taken to the Fingerprint verification module where the users registered fingerprint is matched against the fingerprint obtained from the fingerprint scanner. On passing this, the user is allowed to undertake the test. Fig 1 illustrates the architecture diagram of the system.

To ensure the authenticity of the user during the examination, the system does a fingerprint match on a periodic basis [11]. This is done by dividing the total number of questions into three sections and within each section, for a random question, a fingerprint match is performed. On failing this, the new fingerprint is tested against the database to acquire the details of the person who is helping. After acquiring this, a report is sent to the Controlling Authority with the details of the users involved in the malicious activity. To secure communication between verification module and certification authority server the plaintext is encrypted using RSA algorithm [7].Fig 2 illustrates the algorithm that is devised for the functioning of the system.



```
Algorithm Multifactor Authentication ():
    If Not Registered then
        //Registration Module
        Capture Photo
        Scan Fingerprint
        Get a valid Phone number
        Generate OTP and sent to the Phone number
        If input OTP matches then
            Msg =Encrypt(Phone number, Captured Photo, Fingerprint)
            Msg is sent to C.A.
            If C.A. verifies then
                 Allocate Registered number to the users
            else then
                exit()
        else generate OTP again
    else
        //Login Module
        ID = Getting Enrolled Number from user
        Capture Photo
        If CaptureFailed then
            If Failed count>2 then
                Report
            else
                Capture again
        else
            Encrypted image and ID is sent to C.A.
            If Not C.A. verifies then
                Report
            else
                Scan Fingerprint
                Encrypted Fingerprint and ID is sent to C.A.
                If Not C.A. verifies then
                    Report
            else
                Get a valid Phone number
                Encrypt Phone number and ID is sent to C.A.
                If Not C.A. verifies then
                    Report
                else
                    Generate OTP and sent to the given phone number
                    if input OTP Not matches then
                        Report
                    else
                        //Generate Questions
                        N = No. of Questions/3
                        for n in range(No. of Questions):
                            If n is equal to N then
                            Generate random number between 0 to n =>r
                            If Question attempted is n+r then
                            Scan Fingerprint
                            Encrypted Fingerprint and ID is sent to C.A.
                            If Not C.A. verified then
                                Report
                            Generate the nth Question
                        Repeat
```

Fig. 2 Algorithm

RESULTS AND DISCUSSIONS

The Face Recognition modules extract features such as shape using HOG and use the KNN algorithm to map to the dataset to find the closest face. Fig 3.1 illustrates a student/candidate's face is been captured by webcam. This image has been captured is matched with the corresponding image provided by student/candidate at the time of enrollment with the registration authority. Fig 3.2 illustrates that the two images are matched. If the images don't match, the system gives

3rd International Conference on Recent Trends in Engineering and Technology

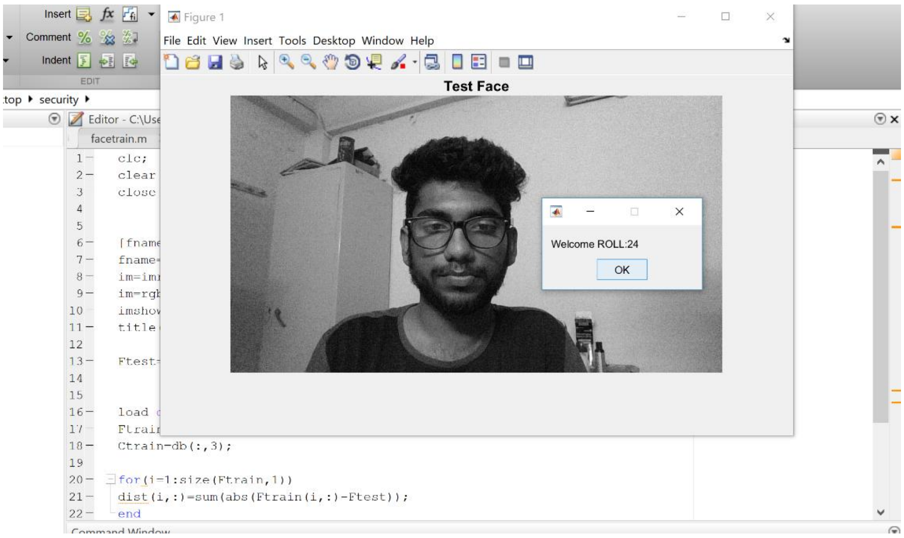
alert by displaying failure. Fig 3.3 illustrates the non-matching scenario. If the Register IDs don't match, the user is denied access.

The OTP module makes use of the Firebase Authentication for logging a user into the system. It involves a mechanism of using FirebaseUI that comprises of a drop-in login widget that executes login flows for mobile number login, along with password-based and associated login. Fig 4.1 illustrates the mobile number been registered receives an OTP.Fig 4.2 illustrates the entered OTP and received OTP are matched. The student/candidate is authenticated by the system. Fig 4.3 illustrates the entered OTP and received OTP is different and hence the access is denied.

The Fingerprint based authentication involves the process of gathering minutiae from the fingerprint input during Registration phase and is stored as a tree structure [5]. Fig 5.1 illustrates the scenario of Fingerprint setup. In the Login Phase, from the input fingerprint fed by the user, a tree structure is computed which is compared against the similar structures stored in the Database. Fig 5.2 illustrates the fingerprint is successfully registered. Fig 5.3 illustrates the fingerprint authentication success. Since fingerprints can have minor variations due to external factors such as distortions, a minimum threshold in a difference between the structures is accepted. Fig 5.4 illustrates the fingerprint authentication failure. In this case, the user is denied access.

A. Face Recognition modules

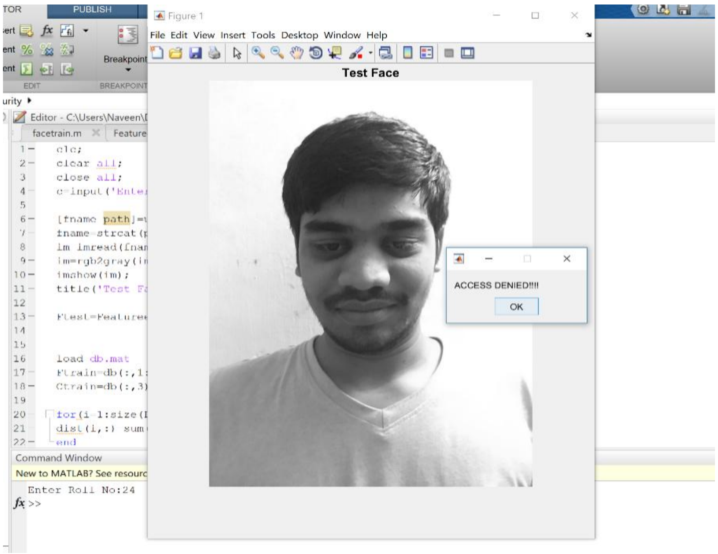
Fig. 3.1 Webcam Image



```
clc;
clear
close


[fname
fname=
im=imr
im=rgb
imshov
title

Ftest=


load d
Ftrair
Ctrain=db(:,3);

for(i=1:size(Ftrain,1))
dist(i,:)=sum(abs(Ftrain(i,:)-Ftest));
end
```

Welcome ROLL:24

Fig. 3.2 Face-Recognition Success


TOR
PUBLISH
Breakpoint
EDIT
BREAKPOINT
Editor - C:\Users\Naveen\[
facetrain.m
Feature
Figure 1
File Edit View Insert Tools Desktop Window Help
Test Face
OK
Command Window
New to MATLAB? See resourc

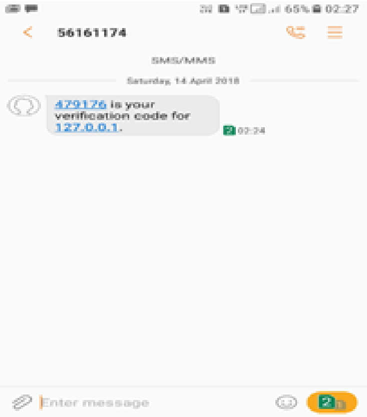
```
clc;
clear all;
close all;
c=input('Ente

[fname path]=u
fname=strcat(p
im=imread(fnam
im=rgb2gray(im
imshow(im);
title('Test Fa

Ftest=Feature


load db.mat
Ftrain=db(:,1:
Ctrain=db(:,3)

for(i=1:size(F
dist(i,:)=sum(
end
```

ACCESS DENIED!!!!

```
Enter Roll No:24
>>
```

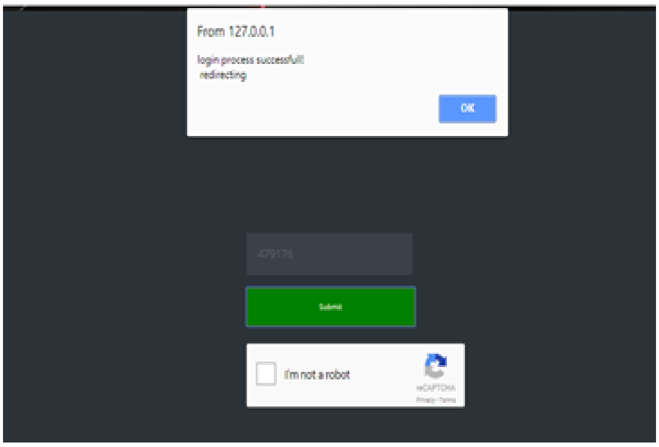
Fig. 3.3 Face-Recognition Failure

B. *OTP Module*



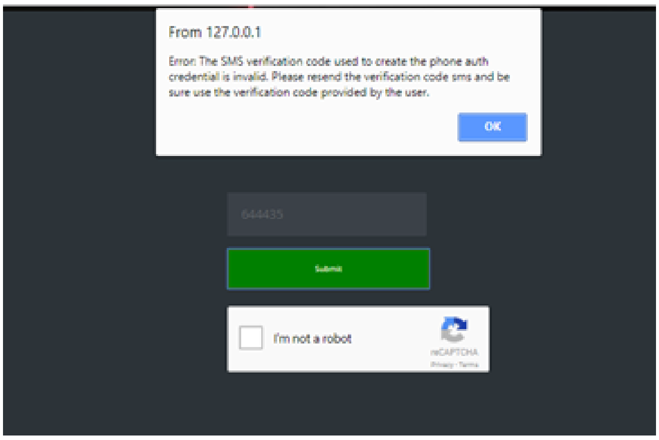
479176 is your verification code for 127.0.0.1.

Fig. 4.1 Mobile OTP Screenshot.


From 127.0.0.1

login process successfull!!
redirecting

Fig. 4.2 OTP Success



From 127.0.0.1

Error: The SMS verification code used to create the phone auth credential is invalid. Please resend the verification code sms and be sure use the verification code provided by the user.

Fig. 4.3 OTP Failure

C. *Fingerprint Module*

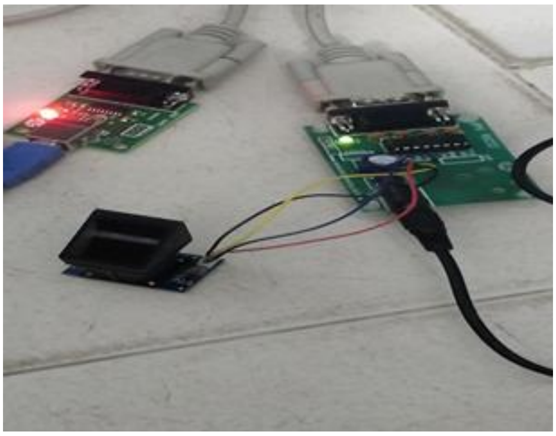
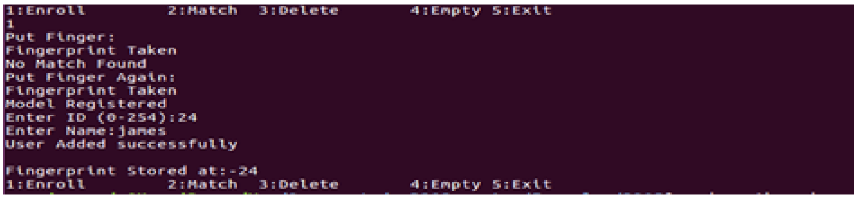
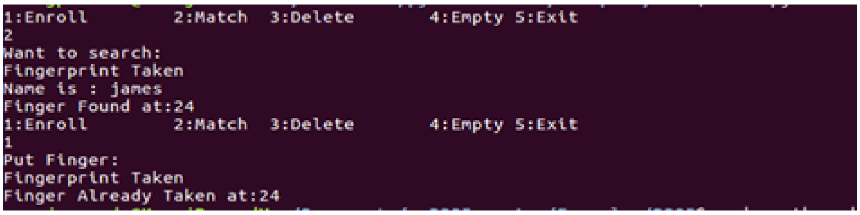


Fig. 5.1 Fingerprint setup



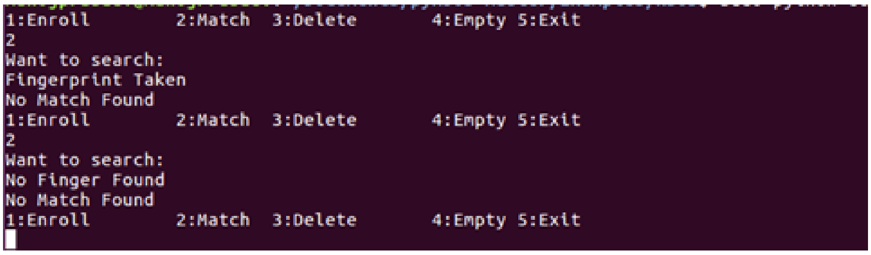
```
1:Enroll         2:Match  3:Delete       4:Empty 5:Exit
1
Put Finger:
Fingerprint Taken
No Match Found
Put Finger Again:
Fingerprint Taken
Model Registered
Enter ID (0-254):24
Enter Name:james
User Added successfully

Fingerprint Stored at:-24
1:Enroll         2:Match  3:Delete       4:Empty 5:Exit
```

Fig. 5.2 Registering Fingerprint



```
1:Enroll         2:Match  3:Delete       4:Empty 5:Exit
2
Want to search:
Fingerprint Taken
Name is : james
Finger Found at:24
1:Enroll         2:Match  3:Delete       4:Empty 5:Exit
1
Put Finger:
Fingerprint Taken
Finger Already Taken at:24
```

Fig. 5.3 Fingerprint authentication Success



```
1:Enroll        2:Match  3:Delete       4:Empty 5:Exit
2
Want to search:
Fingerprint Taken
No Match Found
1:Enroll        2:Match  3:Delete       4:Empty 5:Exit
2
Want to search:
No Finger Found
No Match Found
1:Enroll        2:Match  3:Delete       4:Empty 5:Exit
```

Fig. 5.4 Fingerprint authentication Failure

CONCLUSION AND FUTURE WORKS

The need for a secure Online Examination System has become of immense importance in today's world. The paper proposes a system that employs a face-recognition module, an automatic OTP-generator module and a fingerprint authentication module which on integration enhances the security of the online examination systems. The experimentation clearly revealed the strength of the scheme in terms of mitigating different forms of attacks like resistance to replay, password guessing and parallel session attacks. As a future extension, the team is currently focusing on minimizing the overheads related to network parameters and improving the usability of the scheme with the usage of QR codes instead of SMS based OTP [15].

References

[1] Al-Saleem, S.M. and H. Ullah, "Security considerations and recommendations in computer based testing," in Scientific World Journal,1 September 2014.

[2] Ramu, T. and T. Arivoli, "A framework of secure biometric based online exam authentication:An alternative to traditional exam" in International Journal of Scientific & Engineering Research,Vol. 4,Issue 11, November 2013.

[3] Qinghai Gao," Using IP Addresses as Assisting Tools to Identify Collusions " in International Journal of Business, Humanities, and Technology,Vol. 2,Issue 1, January 2012.

[4] A. Ullah, H. Xiao, M. Lilley and T. Barker," Using challenge questions for student authentication in online examination" in International Journal for Informatics,Vol. 5, Issue 3, September 2012.

[5] AbinandhanChandrasekaran, BhavaniThuraisingham, "Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances," The Second International Conference on Availability, Reliability and Security (ARES), 2007.

[6] N.A. Karim and Z. Shukur," Review of user authentication methods in online examination" in Asian Journal of Information Technology,January 2015.

[7] O. Zughoul, H.M. Jani, A. Shuib and O. Almasri,"Privacy and Security in Online Examination Systems" in IOSR Journal of Computer Engineering,Vol. 10, Issue 4, April 2013.

[8] SwathiPrathish, S.Athi Narayanan and Kamal Bijlani,"An Intelligent System for Online Exam Monitoring" in Information Science (ICIS), International Conference, 2016.

[9] Asha and Chellapan,"Biometrics:An Overview of the Technology,Issues and Applications", in International Journal of Computer Applications,February 2012.

[10] Rudrapal, S. Debbarma and S. Das and N.Kar,"Voice Recogniton and authentication as a proficient biometric tool and its application in online exam for P.H people "

[11] Levy, Y. and MM. Ramim,"A theoretical approach for biometrics authentication ofe-Exams proceedings" in Chais Conference on Instructional Technologies Research,February 2007.

[12] J.Moten,A.Fitterer,E.Brazier,J.Leonard and A.Brown,"Examining Online College Cyber Cheating Methods and Prevention Measures" in Electronic Journal of e-Learning (EJEL).

[13] C.C. Ko and C.D. Cheng," Flexible and Secure Computer-based assessment using a single zip disk" in Computers &Education,April 2008.

[14] N Harini, Dr. T R Padmanaban, C K Shyamala , "Cryptography and Security"

[15] Dr. Harini N. and Padmanabhan, T. R., "2CAuth: A new two factor authentication scheme using QR-code", International Journal of Engineering and Technology, vol. 5, pp. 1087-1094, 2013.

[16] R.Joseph Manoj, M.D.Anto Praveena, K.Vijayakumar, "An ACO–ANN based feature selection algorithm for big data", Cluster Computing The Journal of Networks, Software Tools and Applications, ISSN: 1386-7857 (Print), 1573-7543 (Online) DOI: 10.1007/s10586-018-2550-z, 2018.

[17] G. Indrajith and K.Vijayakumar, "Automatic Mathematical and Chronological Prediction in Smartphone Keyboard" International Journal of Engineering and Computer Science ISSN: 2319-7242Volume 5 Issue 5 May 2016, Page No. 16714-16718.

[18] K. Vijayakumar and C. Arun, "A Survey on Assessment of Risks in Cloud Migration", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.66 May 2015.

[19] K. Vijayakumar,C.Arun,Automated risk identification using NLP in cloud based development environments,J Ambient Intell Human Computing,DOI 10.1007/s12652-017-0503-7,Springer May 2017