Writ Petition Nos.8810 of 2015, 9892 of 2015, 10859/2015, 10860/2015

28.07.2015

Shri A.M.Trivedi, learned Senior counsel with Shri Ashish Trivedi, learned counsel for the petitioner in W.P. No.8810/2015.

Shri Aditya Sanghi, learned counsel for the petitioner in W.P.No.9892/2015.

Shri Amalpushp Shroti, learned counsel for the intervenor.

Shri R.N.Singh, learned Senior counsel with Shri Ajay V.Gupta, learned counsel for the respondent No.31.

Shri Samdarshi Tiwari, learned Dy. Advocate General for the respondents/State.

We appreciate the stand taken by the applicant APDMC that the applicant is committed to conducting transparent, free and fair examination.

Keeping in mind the rival submissions and suggestions given on the previous date of hearing and also after perusing the name of the Agency who is likely to be entrusted with the Online Examination to be conducted for and on behalf of APDMC, in our considered opinion, it may be appropriate to provide for dispensation which may assuage the concern of all the stakeholders and also instill credibility and confidence in the entire process of online examination.

The measures to be adopted as indicated hereinafter are not only regarding the minimum technical compliance to be fulfilled by the concerned Agency but also about the logistical compliances to be done by the principal (APDMC) and the monitoring agency (AFRC). We may consider of issuing directions to provide for following security measures :-

"**Planning to secure Online Examination System Process**

Normally online examination systems must consist of following sections.

(a) Central Examination Server (In which database of all examinee, Question Paper and answer sheet etc.) – 2 Nos. (APDMC and AFRC)
(b) Examination server at each Examination centre
(c) Examinee computers connected with Examination server through LAN.
(d) Network used for communicating with each other.
(e) Monitoring Server - 2 Nos. (APDMC and AFRC)
(f)

Proposed system to enhance security.

The Database Administrator must be appointed from an independent agency such as NIC not below the rank of Scientist C.

A. **Central Examination Server :-**

(1) Should be physically secure. No **unauthorized** and **unauthenticated** access should be given.
(2) **Biometric technology** alongside with traditional password based technology should be used for securing server.
(3) A **replica** of same server should be available with geographically changed location.
(4) Communication between the server should be **encrypted** with best possible technique like RES/MD5 etc .
(5) The owner which has access to each server should be different. Owner of one server should not be able to access the second replica server.
(6) A Monitor server should also be configured in same manner as

of examination server but to store monitoring data such as audio/video/images/biometric data collected from each examination centre.

B. **<u>Examination server at each examination centre.</u>**

(1) Each Examination centre should have **fingerprint reader at main gate** so that only those examinees are allowed whose fingerprint is stored on Examination server in Examination centre. User biometric information (**Fingerprint/face recognition**) may be register at the time of enrollment/form filling through authorized centre or kiosk only.

(2) Each examinee should be validated by his/her own credential (id and password) through the server.

(3) Exam Hall must have auto generated encrypted code for paper. This auto generated code (id) must be distributed randomly. The first candidate who comes in exam room shall have first code, second shall get second code and likewise.

(4) The password of each user stored in the database should be in encrypted form.

(5) As soon as the exam gets over and data is submitted to database on Examination server at each examination centre, immediately the **DML (Data manipulation Language) get locked for the database** so that the data could not be changed at any situation. (Database access time must be limited upto exam period only, whatever it may be 2 hrs or 3 hrs and after examination it must be blocked immediately and no command or deletion, addition, alteration shall be allowed. It is to ensure that the test is taken in a certain amount of time. Some automated testing programs allow this feature). The auto generated id is **for the internal use only** and not be opened to anyone except Examination In-charge having exclusive password..

(6) Each examination hall should have at least two CCTV cameras with audio recording facility to the monitoring server not less than 5 Mhz frequency. The camera must have sufficient electricity back up through UPS, so that the movement and activity of Examinee can be recorded in case of power failure. This data should be uploaded to monitoring server on real time basis.

(7) The recording of desktop of each Examinee computer should also be uploaded to monitoring server on real time basis which in turn to be secured at the monitoring server contemporaneously.

(8) The local server installed at Examination Centre should be connected through VPN to the master server. The internet connectivity on the local server to be disconnected. No possibility

of hacking is possible in this configuration.

(9) The Examination Centre must have ISO 27001 certification.

(10) The Result be declared within prescribed time or within 15 minutes.

(11) The tentative answer keys for the objective type examinations should be hosted on the website of APDMA and AFRC immediately after the examination is over and candidates will be given days' time to file claims and objections, if any to the examination authority.

(12) The same will be placed before the Experts committee of which Database Administrator from independent agency such as NIC is also a member for scrutiny and the corrected final answers be published on the website again. Candidates can self-evaluate their answers with answer keys.

C. **<u>Measures to be taken at Examination Centre</u>**

(1) A firewall like software should be installed to each examinee computer. The task of this software is to remove vulnerabilities present in examinee computer. The tasks are listed as below:-

i. Sync Examinee computer time with server time for effective log maintaining.

ii. All ports except those required for the online exam are disabled and the ports used can be chosen randomly for each examinee; the ports to be used have only to be sent to the examination server at examination centre with the IP of the exam client. Therefore, manipulation through a fixed port can be avoided.

iii. All other programs except the online exam client are deactivated by controlling the inputs of the examinees. By cutting off electronic communications and disabling other computer programs or inputs (including USB ports) on the examinees' computers, the examinees can be prohibited from manipulating their local computer or the Internet. Only mouse should be enabled. The proprietary application software should be used and not to be used the open source software. (It must be ensured that use of google Docs, screen share and opening new window in a separate tab to excess Google must be made impossible. The student cannot use offline material during online examination.)

iv. Desktop recording software is suggested to record all the activity done starting from the exam till the ending of exam on real time basis. (This is very important in the future for cross checking with the answer in main server with actual examinee done at his computer).

v. Online exam access should use **Respondus Lockdown Browser or its equivalent**. The proposed browser module presents to the user at startup a full-screen application window that encases a browser window. However, no address bar is provided, nor are there any menus, toolbars, buttons, or other controls that would be seen on a generic browser. The application window is locked in full-screen mode and cannot be resized or minimized until the application is terminated. Third party software like VNC viewer must be completely prohibited.

vi. **Students id (specific auto generated id link) can work only one question at a time and cannot access completed questions**.

vii. An exam should randomize (scramble) question sequence and answer choices for every id link differently.

viii. One (students) auto generated id link can access the online exam only one time.

ix. The exam should close when the allotted time period for work expires. It is suggested that the exam end should be **triggered by Examination server to all of the examinee computers at once** and not the local time of Examinee computer / browser script should be used.

D. **<u>Network used for communicating with each other.</u>**

i. Communication between the server and Examinee computer should be encrypted with best possible technique like RES/MD5 etc .

ii. Communication between the Central server and Examination Hall server should be encrypted.

iii. The server at examination centre should send the exam data to both of Central Servers on real time basis. (This step is required to prevent fraud at Central Server end or any other Source.)

iv. Every log (Both Database and access log with client unique ID/Timestamp) of each communication between server and Examinee computer should be stored on real time basis for future reference.

(Database log is a log which is created every time when the data (Answer in this case) is inserted into the database with timestamp. Access log is a log which is created every time when the examinee computers access any page of Web server).

<u>Main Feature of proposed system.</u>

(1) A conspiracy/fraud can be detected by cross verifying the answer Sheets thrice through following.

By data available in central server and replica server.

By seeing Desktop recording of particular examinee.

By seeing CCTV video/audio recording of examination room.

(2) As Examinee is being identified by biometric data (fingerprint and face or more) therefore only genuine examinee can attend the examination. It is also verified through examinee credentials."

We are inclined to give some time to both the parties to examine the efficacy of the security measures indicated hitherto and to offer their counter proposal, if any, so that appropriate directions can be issued on the next date of hearing.

We make it clear that if there is any issue about appointing Database Administrator by NIC, the parties may suggest any other independent agency (Government Undertaking) or even names of former Officers of such undertaking not below the rank of Scientist C in NIC or equally qualified.

We accordingly, defer the matter till **03.08.2015** to be taken up at **10:30 AM.**

(A. M. Khanwilkar)
Chief Justice

(K.K.Trivedi)
Judge

AM.