WEB-BASED-SECURE ONLINE NON-CHOICE –BASED EXAMINATION SYSTEM (WONES) using Cryptography

Dr. R. Sheshadri [1] T.Chalama Reddy [2] N.Ashok kumar [3]

[1] Professor and director, S. V. University computer Centre, S. V. University, Tirupati, A.P ,India.
ravalaseshadri@gmail.com

[2] Research Scholar , Department of IT, Narayana Engineering College, Nellore,A.P,India,
chalamareddy.t@gmail.com

[3] Research Scholar, Department of CSE ,QUBA Engineering College, Nellore, A.P, India,
ashok.nadadura@gmail.com

Abstract- Web based Online Non-choice-based Examination System (WONES) is an effective solution for mass education evaluation. WONES ensures transactions between the examination server and the candidates by employing special authentication protocols. This paper proposes an enhanced secured online exam management environment by using Biometric Authentication and One Time Authentication Code (OTAC) by Trusted Third Party monitoring. . A novel feature of the system is its support for formulae and graph input which makes it suitable for non-choice based examinations. There are also a library of comparators which evaluate the difference between the encoded correct answer and the candidate response using heuristic rules.

Index Terms—online exam, secure exam management, the real-time-monitoring system, biometric finger print system, cryptographic protocols.

1. INTRODUCTION

he use of Web-based examination systems is still limited for several reasons. Authenticity of submitted Twork,(which is required to prevent increasingly common legal disputes) is not assured by the Web technologies, as these primarily address issues of confidentiality (e.g. protection ‘of personal details and other sensitive information) rather than ‘authenticity as such. Authentication requires different protocols and different tools, which cannot be derived directly from the secure communication facilities available to the Web. Perhaps more importantly, the greatest disadvantage of some of the current on-line examination technologies is their multi choice nature. During examinations, candidates tick off boxes, select menu items, etc [When less restrictive forms of input are required, candidates often get a text area to fill in, and then the actual assessment is done *post hoc* by a human Teacher. The multi-choice nature of examination is another “security risk” in assessing candidates. Choices can be made on a hunch, by first discarding the least likely alternatives and then taking a gamble on the few that remain’. Another risk factor for reliable on-line assessment is a limited variety of multi-choice questions the Teacher accrues over years, which sometimes makes it attractive for candidates to study samples of a particular exam paper rather than the subject paper that is supposed to be examined.

In this paper we discuss the pedagogical and organizational aspects of the technical solution for secure examinations we proposed earlier [l], when the Web was young, Java had only just been established as its language, and little was known about good practice in on-line examinations. However, since then our system has proven effective in dealing with the drawbacks of online examinations identified above thanks to its combination of examination strategies with advanced Web technology. We refer the reader to paper[1] for any technology aspects that we have no space here to properly explain. The rest of the paper concentrates mainly on technology applications and is organized as follows. Section 2 will discuss the system architecture. Section 3 discusses real time monitoring system. .Section 4 discusses examination evaluation process. Section5 discuses implementation and deployment details. Section 6 explains about conclusions and points to further work are found at the end.

2. SYSTEM ARCHITECTURE

Our WONES is a distributed collaborative system which is based on DCOM Technology, using Enterprise Java Beans (EJB). It has four major components, The Examination Preparation System, The Examination System, The Examination Monitor System and Exam Evaluation which are deployed on JEE (Java Enterprise Edition) Complaint Application Server. We Considered the Open Source JBoss Version 5 Application Server which is Java 5 Enterprise Edition Compatible for Deploying the WONES server side distributed components and MySQL Database Version 5 for Application Storage. The Client Side Components are designed using Open Swings Version 2.3 which is a open source framework. System architecture consists of four sub sections: 2.1. The Examination Preparation System 2.2. The Reliable and Secure examination system 2.3. The Biometric fingerprint system 2.4. Examination system over view.

2.1 The Examination Preparation System

The preparation system is used to manage question storage, assign test ID and schedule the test. The question database is composed of the questions, a set of possible answers, the question types and other metadata, which are indexed by several factors, such as topics, keywords, complexity and difficulty, etc. The database is open to autherised teachers, allowing them to add questions and answers by template.

Teacher role is eligible to create or update Question and Answer Pool (QAP). The QAP is categorized by Course, Subject, and Topic wise which can be created or modified. Teacher has to select the course, subject, topic then the questions list will be displayed (Assuming QAP is created earlier) on the screen with a link to the answer. The Teacher is free to select the available questions or create a new question and the related answer in the QAP.

Since the system is Non-Choice Based, Teacher has to create the Question & Answer for both graphical and non-graphical using the available input methods. Symbols which are required for preparing answer are provided as ICONS which can be dragged and dropped using Mouse in the Graphical Applet. Teacher will place the Icons in the Symbol Panel and draw the Answer in Answer Panel in the Graphical Applet and assign the respective comparators for calculating the differences of the Examinee response.

In QAP every Symbol Icon is associated with a unique code based on the Co-ordinates generated by the Graphical Applet, which is used for encoding the question and answers. Teacher will select a set of questions for test and set examination duration and the questions appearance order (serial/random) and commits the QAP. A unique Examination Code will be assigned for these questions and System confirms the Unique Examination Code generated.

All Unique Examination Codes (UEC) generated by various department Teachers will be displayed as available tests in the Examination Controller/WONES Admin terminal. Every Subject's Teacher confirms the QAP Updation (Only Exam Codes are communicated) to Examination Controller (EC), EC will schedule the tests for the respective subjects according to the notified time table. The exam schedule can be controlled by the Examination Controller/WONES Administrator. Only the registered Examinees for their relative subjects will be able to take the exams in WONES.

2.2 The Reliable and Secure Examination System

Is an online testing interface for students, called WONES, which include the following key features: client side control, time control, security control and auto-installation. Benefiting from DCOM technology, the system can install and update itself conveniently, better than the Client/Server framework. We guarantee the security by cryptography, real-time monitoring and data transmission encryption, randomly asking thumb impression. The cryptography is used to validate student identification before testing. After the environment for the online exam is set up and the examinee is authenticated by using biometric thumb impression, the problem sheet is distributed, and opened for the examinee upon receipt of the message to start the exam.

The workstation runs on Windows Desktop OS called Windows XP. Prior to examinations an account is logged in, which launches WONES Desktop Application which is based on Open Swings Java Framework. The Application window is pre-maximized and overlapped by an additional Java window covering all the

Desktop controls by Password Protection (such as access to Desktop Items or other Applications). This makes it impossible to browse any irrelevant pages, or launch any further applications. All keyboard shortcuts are disabled, too. The displayed window contains the Java Frames for interacting with the student and an invisible Java Process for secure communications, as detailed in the previous paragraph. In the course of the exam, the application window displays panels for questions, answers, symbols and Instructions with options to erase the symbols save or edit the answer. Navigation keys are provided to view the next and previous answered questions.

The problem of candidate authentication for online examination is in a way opposite to the access control problem characteristic of modern e-commerce (For which the Web is specifically geared). Indeed the security risk being prevented is not one of a perpetrator gaining access to a resource intended for a true customer, but one of the true customers secretly and willingly transferring his or her access rights to a spoofer posing as that customer. Here the true customer is a gaining party, and hence it is the system that loses out in the event of security lapse. Password protection simply does not work in this scenario, as the password can be transferred to the spoofer transparently for the system. Protection by certificate, which is the way e-commerce servers protect their customers from spoofers, does not work here either, since certificates, too, can be disclosed by the willing owner. Our security scheme circumvents the risk by introducing a human Trusted Third Party Invigilator (TTPI) to the transaction as follows.

WONES uses a standard Public Key Cryptography RSA Algorithm. A Public Key called One Time Authentication Code (OTAC) is used to encrypt the client and server communication. OTAC is generated at WONES server by Java Key Tool encoded with Examinee USERID, Examinee Finger Print Scanning Information and a secret server side session password while the Examinee is registered. Examinee is hidden with these details while he is registering to WONES. Examine is communicated with registration user id and password details only. The registration data with the assigned OTAC details are stored in the Server Side Security Storage.

TTPI (Trusted Third Party Invigilator) logs in and sends a request for the activation of OTAC for an Examinee from the exam terminal where the Examinee is supposed to take exam. WONES server checks the identity of TTPI by verifying the WONES Clients Digital Certificates and the Location of WONES Client which is already registered at WONES Server Security Storage and activates the OTAC for establishing an open, fully authenticated, bi-directional channel between the Examinee and the server, which is secure to de-facto industrial standards.

This Verification of TTPI credentials and WONES Client's Location ensures that Activation of OTAC for Examinee is protected by unauthorized person access. WONES Client is strictly executed in the Controlled computer lab. As the invigilator is present during this period, the risk of copying is virtually eliminated.

The main idea of PKC is the use of two unique keys for each participant, with a bi-directional encryption mechanism that can use either key to decrypt information encrypted with the other key, as described below:

- **Public key:** One of the keys allocated to each person is called the "public key", and is published in an open directory somewhere anyone can easily look it up, for example by email address.

- **Private Key:** Each person keeps their other key secret, which is then called their "private key".

This powerful architecture has three profound consequences:

- **Geography:** The sender and the recipient no longer need to meet or use some other potentially insecure method to exchange a common secret key. Since everyone has their own set of keys, then anyone can securely communicate with anyone else by first looking up their public key and using that to encrypt the message, enabling secure communication even across great distances over a network (like the Internet).

- **Digital signatures:** A sender can digitally sign their message by encrypting their name (or some other meaningful document) with their secret key and then attaching it to a message. The recipient can verify that the message came from the sender by decrypting their signature with their public key. If the decryption works and produces a readable signature, then the message came from the sender because only they could have encrypted the signature with their private key in the first place.

- **Security:** The disclosure of a key doesn't compromise all of the communications on a network, since disclosure of public keys is intended, and only messages sent to one person are affected by the disclosure of a private key.

2.3 The Biometric Fingerprint System

Biometrics consists of automated methods of recognizing a person based on unique physical characteristic. Each type of biometric system, while different in application, contains at least one similarity.

The biometric must be based upon a distinguishable human attribute such as a person's fingerprint, iris, voice pattern or even facial pattern. Fingerprints are the most commonly used biometrics solution as they are less expensive compared with other biometrics solutions.

In the present market computers are available with inbuilt biometric devices like fringer print scnner and iris etc. For example, some laptops are equipped with it and also with a biometrics mouse. This devise is part of a package of fingerprint authentication mechanism.

The mouse is about the same size as standard mouse, however, it also has an integrated fingerprint scanner that is managed by client side software and controlled by server side software centralized on an authentication server.

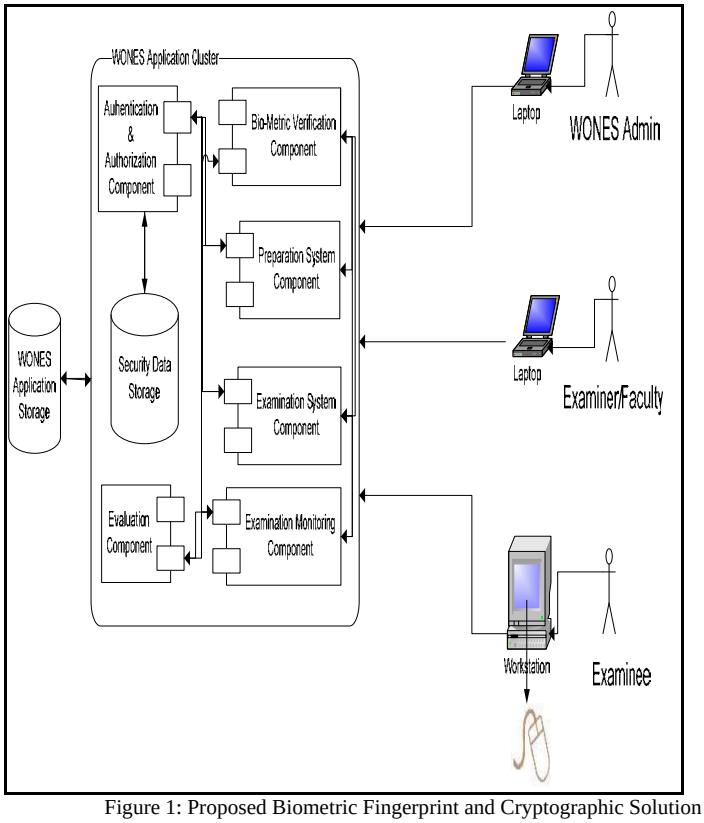


Figure 1: Proposed Biometric Fingerprint and Cryptographic Solution (WONES) For E-Exams

2.4 Examination System over view

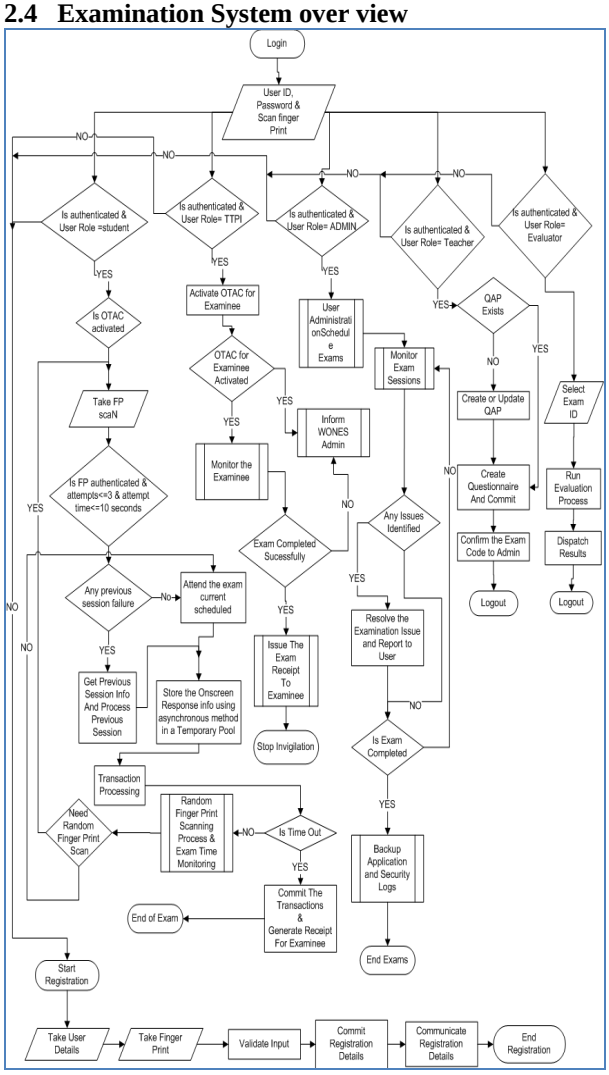


Fig2: WONES Flow Chart

As shown in figure2 WONES contains the logic for attending exams by Examinee, Invigilation and OTAC Activation by TTPI, User Administration by WONES Administrator, QAP and Questionnaire creation by Teacher and Results Dispatch by Evaluator.

This Examination logic is described as follows:

- All Examinees need to be registered with their Finger Print Scanned. Whoever fails to register will be redirected to registration process.
- Examinee can take up examination by entering login id and password along with Finger Prints Scanned and after OTAC activated by Invigilator.
- If Examinee is a registered user for the exam being conducted and had faced any error or failure (due to hardware or network problem), while exam is under process, user can continue the exam once the system is recovered within the period of time.
- Examinee needs to scan his/her Finger Prints in between the Exam at Random intervals; however a minimum time and countable attempts are given as discount for this repeatable process from the given Examination Time.

- During the answering process to every question all on screen activities are recorded in a temporary storage asynchronously to help the candidate for maximum recovery from system failures. All the transaction will be committed with No-Rollback Flag in the system once the given exam time is completed. Examination Window Closes without any warning to Examinee and confirms his/her Exam receipt, which has to be collected from the invigilator.

User Administration:

In WONES the users are centrally organized by the WONES administrator and the WONES Administrator is created at the installation of WONES. The WONES users are categorized by their roles. Following are the roles present in WONES. Every user in the WONES are registered with valid identification details along with their Biometric finger prints under the control of WONES Admin.

ROLE 1: Teacher
ROLE 2: Examination Controller (EC)
ROLE 3: Invigilator (TTPI)
ROLE 4: Examinee
ROLE 5: WONES Admin
ROLE 6: Evaluators

Teacher: Will prepare Questions and Answers for the related subject. Will Prepare the Question Paper for Examinees with parameter like *exam duration, number of questions, questions ordering* (RANDOM/SERIAL), *max marks, answer validation related comparator from the comparator library.*

** Questions that are created by Teacher of the same department/subject are only visible from the QAP.

Examination Controller: Will notify the WONES users for examination registration with a time table. EC selects the available papers with Unique Exam ID for examination schedule. All the parameters like *Exam Code, Exam Type* (Internal, External), *Exam Duration, Exam Start Time, Exam end Time* are set by him. Exam Duration is always cross verified with the Questionnaire prepared by Teacher.

Invigilator: Will act as a Trusted Third Party Invigilator (TTPI) in the controlled and supervised computer lab for conducting the online exams. He Identifies the Examinee with Valid proof of identity with the Examinee user ID (registration code) and Finger Prints taken through Finger Print Scanner. He then facilitates the Examinee for One Time Authentication Code (OTAC) Activation at Examinee terminal where he/she is supposed to attend the exam. Invigilator monitors the candidates that they are not involved in any cheating activities.

Examinee: Will attend the exam in a controlled computerized lab where WONES is installed. Examinee has to submit his Valid ID proof and the WONES registration details. Examinee has to enter his WONES user ID and password along with his finger prints for OTAC activation process in order to continue for attending the exam. After Exam, Examinee has to collect the Receipt delivered by WONES from TTPI.

WONES Admin: Will administer the users. Activating, deactivating, monitoring the examination sessions.

Evaluators: Will run the automated or Manual evaluation process and get the results reports generated. Will dispatch the results to the concerned departments, and to the Individuals.

3. The real-time monitoring system

The Real Time Monitoring System includes the WONES Admin and Trusted Third Party Invigilator (TTPI) who are Registered Users with their Bio-Metric Finger Prints Scanned. It also requires students not to leave the computer during the test. The data transmission encryption system transmits the examination question and answer in secret form through the network to the server. The examination monitor system is also the manager of the examination system, by which it monitors person's fingerprint randomly for the processing the Exam safely and securely.

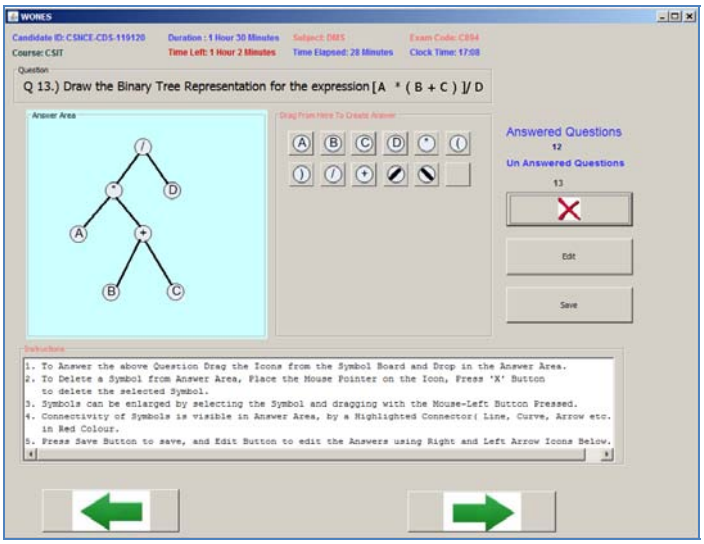
4. Examination Evaluation Process

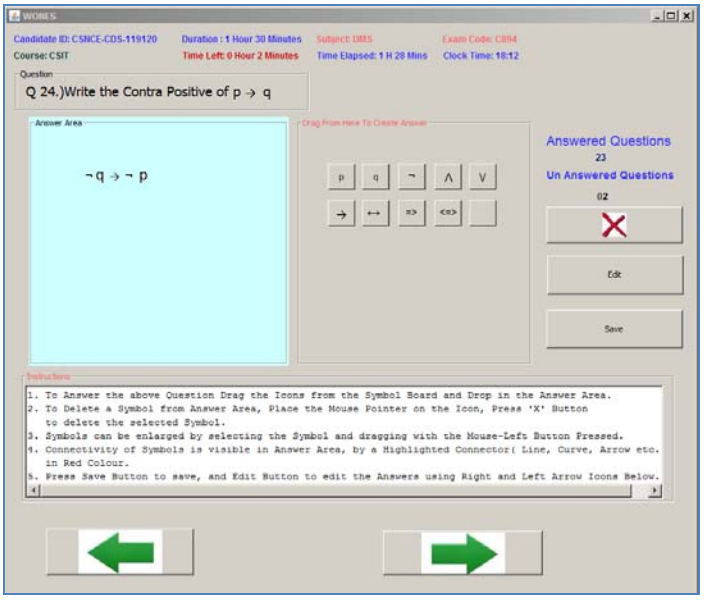
This is an automated process which is run by Evaluator. Since the QAP contains the encoded answers for the Questions, A set of Comparators are used to evaluate the difference between the encoded correct answer and a candidate's response using heuristic rules.

The answer created by Teacher is an encoded output generated by Graphical Applet, a set of graphical comparators are been used to compare the differences of Examinee's Answer and Encoded Correct Answer.

For example, there is a rule for quantifying the difference between two sets, which was used with the graph applet. The set of edges in the correct answer was symmetrically subtracted from the set in the candidate's answer and the cardinality of the result was determined. Full mark was given for zero difference, half of the full mark for difference in one element, etc. These numbers are parameters to the library module "set comparator".

The Following figures depicts the usage of WONES in a better way.





As the repertoire of the applets broadens, further comparators may be introduced to effect the specific pedagogical criteria for assessment in a particular area.

It should be noted that all forms of multi-choice input produce text-encoded results. In the case of formula input, each building block has a sequential number and the answer is a sequence of these numbers. In the case of graph input, each edge is characterized by a pair of vertices, i.e. numbers. All the pairs are collected into one set, which is then sorted (to prevent multiplicity of representation) in some order. Applets implementing simple choices note the sequential number of the choice being made. There is also a "Submit" applet that sends the complete collection of choices gathered from other applets to the communication applet for forwarding to the server.

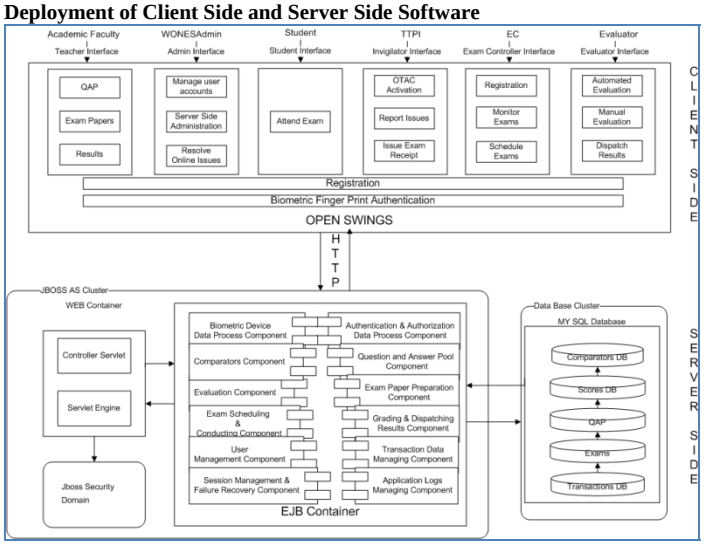
5 Implementation and deployment details

JBoss Application Server Version 5 (JBoss AS is a Java Enterprise Edition 5 – compliant application server) is used for Server Side Application Management. A Java application server standardizes the application development architecture. It does this by defining several component models—standards that developers can use to develop components. These components can be deployed into an application server using a standard deployment model. When the components are running in the server, the server provides a set of services that are made available to the components.

The application component models include standards such as Enterprise Java-Beans (EJBs), Java Server Pages (JSP), and servlets. Some examples of Java EE services that are available to these components include remoting, security, transaction management, persistence, messaging, resource pooling, concurrency control, naming and directory services, and deployment.

WONES server side components are deployed in JBoss EJB Container for interacting with the WONES clients remotely. WONES provides web interface for Admin, Teachers, Evaluators, which is launched from server side. Controller Servlet will process the requests by establishing the communications with WONES Clients and WONES Server Side EJB Components. All security data for establishing secured communication with clients will be in the control of JBoss security domain.

Deployment of Client Side and Server Side Software



Key Design Principle and Patterns Incorporated

WONES utilizes lot of major design patterns and principles. This section describes some of the major design patterns used in WONES. Throughout the application, we have used the principle of programming to an interface, which allows design to be completely decoupled from implementation. For example, for testing purposes, we can replace a heavy database implementation with a lighter-weight mock implementation. Use of an interface also leads to dynamic binding and polymorphism, which is consequentially important to object-oriented programming.

Model View Controller Pattern

MVC is an architectural pattern used in software engineering. The pattern isolates "domain logic" (the application logic for the user) from input and presentation (GUI), permitting independent development, testing and maintenance of each.

WONES has its presentation layer (View) implemented in OpenSwings, which is a Java based Open Source Frame Work. The Model layer is developed using Enterprise Java Beans- EJB integrated with Persistence Layer implemented in MySQL Database. All the EJB Model Components are deployed in EJB Container of JBoss AS. The Controller Layer contains *Controller* Servlet provided by OpenSwings framework.

WONES View is launched by installing the WONES Client at the Workstation as explained earlier. The *Controller* Servlet is a server-side controller for all HTTP requests generated in the WONES client-side is deployed in JBoss web container which is an in built Apache Tomcat Web Server. The Servlet includes a database connection system to MYSQL Database that can be customized and a user authentication system. This component can be integrated with one's own server-side framework, such as Springs, JSF, etc.

Front Controller Pattern

The Front Controller pattern defines a single component that is responsible for processing application requests. A front controller centralizes functions such as view selection, security, and templating, and applies them consistently across all pages or views. Consequently, when the behaviour of these functions needs to change, only a small part of the application needs to be changed.

The Front Controller design pattern is applicable and useful for all kind of applications be it web or desktop applications and is not limited to any single programming language or framework. Before the rollout of MVC frameworks in the market, the design pattern was still in use. The only downside was that not all application could make use of it because of the effort involved. Only the applications which had custom framework in place were using the design pattern.

Asynchronous Commit

Committing to a database is usually a synchronous operation. In other words, the client that requests to persist a data waits till the data has been fully committed. In a typical examination situation, maximum users would be committing their result in a single point in time i.e. at the time when the exam time is over. Also in a typical Non-Choice Based Exam, all the onscreen information (which is also used for Maximum recovery in the instance of unexpected failures) is large in the order of 10^2. This produces a performance bottleneck as all clients would be required to wait until data is persisted.

WONES asynchronously save the Desktop Events (Onscreen Info) into a Local Cache on the Client Side Machine using AJAX Technology. This is info is stored in a non-readable format and is processed by the WONES Server Side Components only. This technique helps the clients to recover speedily to the previous state whenever a failure is occurred, where the failure may be a Hardware specific, software specific and for Committing the GUI data to the Remote MYSQL Database.

6. Conclusions and future work

This paper demonstrates the utility of secure, flexible examination systems in the practice of higher education. This paper is useful for conducting non-choice based examination in subjects like data structures, Discrete Mathematical structures, formal languages and automata theory etc .Although a proper empirical study of the effectiveness of on-line examinations was not made (and none is available in mainstream literature even now), the subjective feedback was very encouraging.

Three issues should be addressed in future work. Firstly, more extended choice applets should be produced to cover a wider spread of subjects. It would be interesting to attempt subjects such as finite automata and graph theory to enable a broader evaluation of the proposed technology.

Secondly, the textual descriptions of the questions and expected answers are exceedingly cryptic where randomization and multiple input forms are being used. Now that XML is the de facto standard for management of structured data, it would be desirable to develop an XML schema for all forms of examination material.
Thirdly, the most costly part of exam design is preparing the actual questions. It would be a great advantage if GUI support were available for this activity. This comment applies to both the questions themselves and their expected answers with the appropriate comparator specifications.

Future research may be fruitful by examining student's attitudes and psychological aspects associated with the proposed solution of e-exam user's authentication. Furthermore, future research may look at the economical issues associated with implementation of such solution

REFERNCES

[1] D.B.Barsky and A.V.Shafarenko. WWW and Java-based distributed examination system for distance learning applications. Aizu International Symposium on Parallel Algorithms/Architecture Synthesis, 1997.
[2] Magdi Z. Rashad, Mahmoud S. Kandil , Ahmed E. Hassan, and Mahmoud A. Zaher (2010), "An Arabic Web-Based Exam Management System", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10 No: 01. Page 48-55.
[3] Yair Levy and Michelle M. Ramim (2007), "A Theoretical Approach for Biometrics Authentication of e-Exams", Nova Southeastern University, USA. Page 93-101.
[4] Yuan Zhenming, Zhang Liang, Zhan Guohua (2003), "A Novel Web-Based Online Examination System For Computer Science Education", 33rd ASEE/IEEE Frontiers in Education Conference, S3F-7-S3F-10.
[5] Ibrahiem M. M. EL Emary and Jihad. A. A. Abu Al Sondos (2006), "An Online Website for Tutoring and E-Examination of Economic Course", American Journal of Applied Sciences 3 (2): Page 1715-1718, ISSN 1546-9239.
[6] D Carlson, M Guzdai, C Kehoe, V Shah, and JStasko. WWW interactive leaming environment for computer science education. SIGCSE Bulletin, pages 290-294, 1996.
[7] C.-R. Jordi, H.-J. Jordi, and D.-J. Aleix, "A secure E-exam management
[8] system," in *Proc. 1st Int. Conf. Avilabil., Reliab. Security*, 2006.
[9] Y. Zhenming, Z. Liang, and Z. Guohua, "A novel Web-based online examination system for computer science education," in *Proc. 33rd ASEE/IEEE Frontiers in Educ. Conf.*, 2003, pp. S3F_7–S3F_10.
[10] D. M. Eplion and T. J. Keefe, "On-line EXAMs: Strategies to detect cheating and minimize its impact," in *Proc. 10th Ann. Technol. Conf.*,
[11] C. Rogers, "Faculty perceptions about e-cheating during online testing," *J. Comput. Sci. Colleges*, vol. 22, no. 2, pp. 206–212, 2006.
[12] D. L. McCabe, L. K. Trevino, and K. D. Butterfield, "Cheating in academic institutions: A decade of research," *Ethics Behav.*, vol. 11, no. 3, pp. 219–232, 2001
[13] [12] A. Shafarenko and D. Barsky, "A secure examination system with multi-node input on the world-wide Web," in *Proc. Int. Workshop on Adv. Learn. Technol.*, 2000, pp. 97–100.
[14]. J2EE: The Complete Reference by James Edward Keogh
[15]Mastering E09. Professional Ajax: Nicholas C. Zakas, Jeremy McPeak, Joe Fawcett
[16]JB 3.0 4th Edition By Gerald Brose and Rima Patel Sriganesh.
[17]. Java Design Patterns: A Tutorial By James William Cooper

Dr.R.Seshadri Working as Professor & Director, University Computer Centre, Sri Venkateswara University, Tirupati. He completed his PhD in S.V.University in 1998 in the field of " Simulation Modeling & Compression of E.C.G. Data Signals (Data compression Techniques) Electronics & Communication Engg.". He has richest knowledge in Research field. He is guiding 10 Ph.D in Fulltime as well as Part time. He has vast experience in teaching of 26 years. He published 10 national and international conferences and 8 papers published different Journals.

T.Chalama Reddy Working as Professor in Narayana Engineering College, Nellore . He completed his M.Tech in J.N.T.University in 2000 in the Specialization of "Software Engineering". His interested area is Networks Security and Cryptography .He has vast experience in teaching of 16 years. He published 3 national and 1 international conferences and 2 papers published different Journals.

N. Ashok Kumar, studying in M.Tech (Computer Science and Engineeing) in QUBA College of Engineering ,Nellore. His interest area is Networks Security and Cryptography. He published 1 national conference Paper.