Secure E-Test Scheme

Mohammad A AL-Fayoumi [1], Sattar J Aboud [1] and Mamoun S. AL Rababaa [2]

[1] Middle East University for Graduate Studies/Faculty of IT, Amman, Jordan

[2] Al-al Bayt University/Department of Information Systems, Amman, Jordan

***Abstract*—E-test is that test performed over the internet in which questions and solutions are computer files rather than sheets of paper. The application of e-test as a perspective knowledge measurement is apparent. But, security for such scheme is not obvious. Thus in this article we introduce a secure e-test scheme with wireless networks. In addition, we suggest a swapping technique between test application and test security. The main contribution of the proposed scheme is to overcoming of the limitations in the milieu trust system. We are claimed that the proposed scheme is efficient and more flexible than the milieu trust system.**

***Index Term*—e-test scheme, wireless technology, e-test security, public key encryption**

I. INTRODUCTION

E-learning is the utilization of internet, software and any other e-media to combine the power of all the new technologies in order to enhance the learning process [1].

E-.learning presents a different method of learning that can assist participants in many ways. Every participant can access a considerable amount of data, study in their self-base, be more certain, communicate with colleague classmates, and they will release from the conventional classrooms pressure.

However, e-learning is not intended to substitute the classroom learning. It may be employed to combination with more than one traditional learning way; in this case the term blended learning is employed. E-learning platform offers many services. Some of these services are common and is raised since computers were first used in education, the other services can vary from one platform to another. One of the most important services for any e-learning platform is the e-testing service. Such service gives access to e-testing information when it is needed in which presents entirely on the internet [2, 3]. Their technical constructions rely on the integration of wireless technology, communication tools and computer system, to help professionals in remote e-testing scheme [4].

There are many different ways to utilize the e-testing scheme. In all cases is important to generate a balance between the benefits and the costs coupled with this technique [5]. The sort of questions and solutions should utilize the extensive ability of the internet and the needs for the participants are main issues to judge.

Some research paper suggested that the infrastructure for e-testing scheme requires the construction an e-testing center [6]. A testing centre should act as the central point for all e-commerce testing services [7]. E-testing center is referred to as e-testing mall. The testing center site must be designed as a virtual campus that houses free and for fee e-testing services. The purpose of this article is to develop a secure e-test scheme in which questions and solutions can perform through this mall.

However, various methods can be used to describe e-test scheme. We develop an idea of the e-test scheme which is executed by a program file and that gives a test solution which is saved in an e-file. The great characteristic of e-test scheme is that the questions and solutions are in e-platform. This reality has important involvements regarding handling e-test resources.

II. RELATED WORK

So far, the Consortium I.G.L is the first one suggested e-test typed scheme [8], in which the test assessment can be computerized and the result is calculated once the participant completing the test. The advantages of e-test scheme are significant in the e-learning or virtual learning environment in which instructor, participant and the colleges are linked employing wireless technology. In addition, containing test data in e-platform ease the entire data handling.

However, e-test is implemented inside the virtual model, which is hard to perform because the difficulty of control and the complexity of participant authentication. Actually, e-test scheme should guarantee that the valid participant is the only one who answers the questions. For this reason, virtual e-test schemes used now are based either on a milieu trust system, or on a participant trust system [9]. In the participant trust system participant should not deceive and must pursue the regulations correctly. This system in certain situations is not a practical system because participant trust can not be unspecified. Actually, participant ignores the trusted participant system since outside community academy recognition [10].

The milieu trust system for virtual e-test requires a trusted physical location so that the participant can take the test [11]. In addition, the computer and platform employed in e-test scheme are trusted in the milieu trust system. These limitations decrease significantly the possible realism of e-test scheme even if, security goals are reached.

In this article we suggest a secure e-test scheme. The suggested scheme allows participant to have e-test in a milieu trust system employing wireless technology in order not to base on predetermined infrastructure. The suggested secure e-test scheme can be applied in a mobile e-test laboratory that is installed without cost and without communication requirements. This characteristic is very significant for pure e-testing colleges that are not have any predetermined real infrastructure and no need for lease houses in order to perform their participant e-test. The aim

of the proposed scheme is to conquering of the limitations in the milieu trust system. The proposed scheme is efficient and more flexible than the milieu trust system.

III. THE OVERALL SCHEME

First we present the notations used in this paper:

g : Generator of a multiplicative group

$test(q)$: Test questions

$test(s)$: Test solution

m : The message to be signed

$h(m)$: One way hash function

r_1, r_2 : A random positive integer numbers

e_1 : Public key for test computer

e_2 : Public key for test server

d_1 : Private Key for test computer

d_2 : Private Key for test server

$cert_1$: Test computer certificate

$cert_2$: Test server certificate

Id : Participant identification

t : Present time

The proposed scheme is designed to be employed in a standard classroom using a wireless access point linked to a server that is test server. If the classroom has wired communication, the server could be located in the network, but if not the server could be located in the classroom linked to the access point. In addition, each participant is supplied with a test computer and a wireless card. However, test computers are not requiring installations. As e-test requires an internet communications the greatest flexibility for that communications is the utilization of mobile service and wireless technology. When the connection between test computer and test server is achieved by wireless technology, mobile e-test laboratory is guaranteed because no communications is wanted in the classroom where the test is occurred. The general e-test scheme is shown in figure 1.

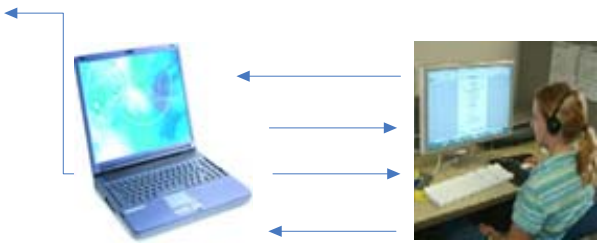


Figure 1. The general e-test scheme

However, the proposed e-test scheme begins once the participant selects one of the test computers to set the test. The participant authenticates to the test server by the test computer employing the authentication scheme (step 1a and step 1b). Then, the participant is allowed to get the test.

As soon as the test time starts, the test server performs the test download scheme (step 2) whereas test questions, $test(q)$ are passed to the test computer. Participant has the limited time to answer the test. After the participant completes the test, test solution $test(s)$ should be passed to the test server. Before passing the test solution, the participant implements the test registration scheme (step 3) for getting a time-stamp over the test solution $h(test(s))$. The time-stamp is checking the accepted test solutions with a covered time if certain difficulties happen throughout its transfer. The test upload scheme (step 4) passes the test solutions to the test server then the test server returns a signal receipt. Lastly, test questions and solutions will remove from the test computer.

IV. SCHEME DESCRIPTION

The suggested scheme consists of two parts which are the following:

A. The Elements

There are three elements in the proposed scheme which are the following:

1. *Participant*: The individual that needs to take the test. The major step for participant is certainly the authentication scheme. Since the authentication scheme employs public key encryption, participant should have two keys that are a public key and a private key and a certificate publish via a trusted authority. Many algorithms can be employed to allow participant to achieve the authentication scheme.

2. *Test server*: is the computer that does the entire operations through the test. Its job is the same job of the instructor in classroom test. It is accountable for participant authentication, care of test questions and solutions and also for the time test monitor. The test server requirements are as follows:

- Should own sufficient space memory to deposit the entire set of test questions and solutions
- Should be capable to achieve participant authentication
- Should give a time-stamp facility to roll the test
- Should supply concurrent test computer links by a mobile device.

3. *Test computer*: is the computer that the participant utilizes to solve the questions. The test computer requirements are as follows:

- Should allow participant to solve test questions. This specifies the sort of device based on the test design. For example, a multi choice test can be performed over PDA, whereas an ordinary test is achieved in a notebook computer. Also, if the test is hand written, a personal computer could be employed.
- Should communicate with the test server. This communications require test computer to be supplied with wireless card, for example a notebook card.
- Should enable participant to validate in opposite of the test server. Also, participant can provide test computers all data required in the authentication scheme such as password. The authentication scheme will be done via a participant mobile device. Therefore, test computer must be able to communicate with the participant mobile device [12].

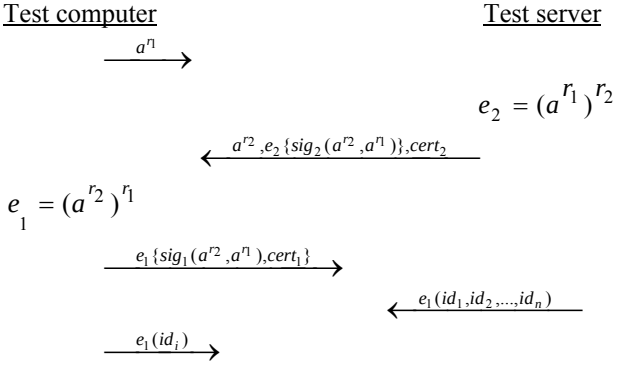
B. The Schemes

There are four schemes in the suggested protocol which are as follows.

1. *Authentication Scheme*: is the core of the entire system. Its services are related to the security standpoint because this scheme can permit or can not permit participants to attend the e-test. Participant Authentication can be achieved in by means of various techniques but for the suitability of this scheme we employ a secure public key authentication scheme [13]. The scheme suggested relied on public key encryption that gives robust to the authentication scheme. This denotes that each participant should own two keys one for public key and one for private key. However, the suitable authentication scheme is the mutual authentication scheme [14] which relied on the Diffie-Hellman key exchange scheme [15]. This scheme is a three passes Diffie-Hellman scheme which sets up a shared session key between the test server and the participant. Lastly the participant is authenticated face to face with the test server. The test sever is also authenticated face to face with the participant. The authentication scheme is illustrated below. Suppose that the test computer work on behalf of the participant and the participant supplies certain data such as secret keys if needed. Therefore, the steps of the scheme are as follows:

- Test computer chooses a random generator a of a multiplicative group since the discrete logarithm is difficult to solve. After that it selects a random challenge r_1 and then sends a^{r_1} to the test server.
- Test server chooses a random challenge r_2 and then finds the key $e_2 = (a^{r_1})^{r_2}$. Then calculates a^{r_2} and signs (a^{r_2}, a^{r_1}) using its secret key d_1. The finding signature is encrypted by Elgamal encryption scheme [16] using the key e_2 produced above. Then together the result of a^{r_2} and the test server certificate $cert_2$ with the encrypted result of the signature are all passed to the test computer.
- Test computer calculates first the key e_1, gets and authenticates the digital signature. Then sign (a^{r_2}, a^{r_1}), using its secret key d_2 and then encrypts the value of signature and the certificate $cert_1$ using the key e_1. Then checks both test server and participant. If so, then accepts, otherwise rejects.
- Test server passes to the test computer the identification *Id* of all participants taken the test in the classroom. The identification *Id* holds data related to the test such as test topic, time of the test, and so on.
- Test computer send to test server commits that the test is taken

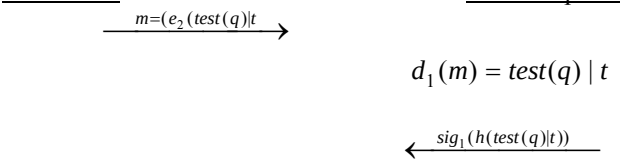
However, the information flows in authentication scheme are as follows:



2. *The test download scheme*: The steps of the scheme are as follows:

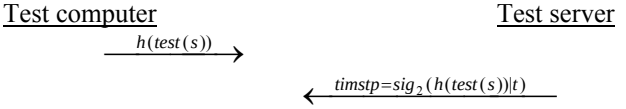
- Test server sends test questions, $test(q)$ to the test computer. The data passed should encrypt with the key e_2 so that to guarantee test server validation. Then computes the message $m = e_2(test(q) \mid t$ which includes the present time t.
- Test computer recovers the message m by computes $d_1(m) = test(q) \mid t$. Then signs the test questions using hash function h pursued by the authentication tag as follows $sig_1(h(test(q) \mid t))$. Then the signature sends to the test server as a signal to confirm the start of test time.

Then, the information flows in test download scheme are as follows:



Note that once this scheme functioning, the participant has the test questions in his computer and commences to solve the questions

3. *The test registration scheme* is executed as soon as the participant completed the test and prior to the test is passed to the test server in the test upload scheme. The test registration scheme is a time stamp service that guarantees integrity of the facts related to test solution $test(s)$ in a known time. The time-stamp scheme works as follows. The participant passes the facts being time stamped and the time stamp returns true. Then, the information flows in test registration scheme are as follows:



There are many time stamp services are available [17, 18] and we can utilize any one from them. While the registration process is executed through the test upload, we perform it in advance to employ a typical timestamp scheme. In addition, the test solution file length may result

burden network difficulties throughout the test upload. For example, a normal test with 100 participants passing every test records at one time produces around 30 Mb traffic, consider that two pages written test produced by a personal computer needs 120 kilo-bytes in average. Employing the test registration scheme prior to the upload, it is required a standard of 160 bit hash function to guarantee what the participant answered until the finishing test time. As soon as test solution is time stamped tests are uploaded yet subsequently the test finishing time preventing network burden.

4. *The test upload scheme*: the steps of the scheme are as follows:

- Test computer passes the test solution to a test server encrypted by the key e_1 .
- Test server recovers the message. Then finds the hash function of the obtained data and verifies it with the hash function outcome formerly time stamped. Then the test server passes a signal receipt to the test computer.
- Test computer erase questions and solutions from the computer.

However, the information flows in test upload scheme are as follows:

Test computer — Test server

$\xrightarrow{m=e_1(test(s))}$

$d_2(m) = test(s)$

$h(test(s)) = h(test(s))$

$\xleftarrow{ok}$

V. SECURITY FEATURES

As we mentioned previously in this article the proposed e-test scheme follow the milieu trust system. This indicates that each device employed in the proposed scheme is a trusted device. This is significant because limitations on the links between test computers and other systems are entirely controlled. In addition, owning test computer as a trusted device means that potential threads from these devices are impossible because the test time that will give to a participant to fraudulent the test computer is in fact very little. However we will discuss each scheme included in this article related to security point view.

A. The Authentication Scheme

The proposed authentication scheme contains many security characteristics. These characteristics obstruct various potential attacks for example content verification attack, content codebook attack and content substitution attack [19, 20]. Though, these characteristics are as follows:

- Mutual authentication: since a test computer and a test server should validate every other via the certificate and via the digital signature scheme.
- Real test: test authentication is essential because the participant should be certain that the test he is received is a right one presented through the authentic test server.
- Key generations: the authentication scheme generates a shared key between both participants. This shared key is employed to secure the communication channel between a test server and a test computer. However, key generation is done via mutual key agreement, thus combined mutual key authentication and mutual key freshness are supplied.
- Participant identification privacy: privacy is given versus an overhearing attack, because data of identity is enciphered using the shared key prior to its sending.

B. Test Download Scheme

The test download scheme employs public key encryption scheme such as RSA scheme to validate the test computer. Actually, this decreases the time cost of the test server because preclude exponent key calculations. The key string employed in this scheme is not required to be lengthy, yet for authentication uses, because the time gap between the authentication scheme and the test download scheme is on average small. Test download scheme also checks the opening time of the test. Observe that the participant signs the hash function of the test pursued by a time tag. This authentication verifies that the participant begins with specific test at a known time. The key security problem is that participant must not be competent to contact or chat with any one throughout the test.

C. Test Registration Scheme

Security of test registration scheme is easy to achieve since a typical time stamp method is employed to register a test. Observe that the scheme finishes by a registration acknowledgment of test result hash function. This acknowledgment confirms that the precise test solution content at the end of test period.

D. Test Upload Scheme

The test uploads scheme permits the test to be sent to a test server. Integrity and privacy of test solutions is guaranteed because cryptogram between test computer and the test server is encrypted by the shared key produced throughout the authentication scheme. In addition, test solutions integrity with report of file solution produced at the end of test time is also guaranteed. Observe that the test server audit hash result of the obtained test solution whether is congruent to the preceding hash result or not. This technique reflects that every participant should have the same time to end the test and the time is not relied on who upload the test initially.

VI. CONCLUSIONS AND FUTURE RESEARCH

It seems that e-test activities have become an important force in e-learning. Its ability can be seen in providing to distributed participant at different sites and zones and at different time its services to make it interested to professionals and participants. E-test scheme needs significant investments in time and funds, both to enhance scheme from time to time concerning revised questions and solutions. The research results must assist the professionals, and policy creator of universities to recognize the areas of e-test they can invest to earn efficiency and cost savings in remain test schemes.

In this article the secure e-test scheme employing wireless networks is introduced. The proposed e-test scheme pursues the milieu trust system. The main contribution of our scheme is to overcoming of the limitations in the milieu trust system. We are claimed that the proposed scheme is more efficient than the milieu trust system

This denotes that each device employed in the proposed scheme is a trusted device. However, this may appear a constraint. Mobile technology and wireless devices permits authors to generate a mobile test laboratory that may be simply installed in any classroom.

Future research can be concentrated in maximizing test applicability with preserving the same capability of protection. By permitting test computer be un-trusted device, then participant can use their notebook to sit and take test. In addition, the areas that need future research may include, simulation scheme, real time protocols, intelligent tutoring, behavior analysis of participants, copyright protection and authentication mechanisms and other issues of e-testing in which still need researching, professionals and participants to work together to make this modern scheme more successful.

REFERENCES

[1] Whille C., Dumke R., Abran A., and Desharnais J., "E-learning Infrastructure for Education", International Conference of the IASTED 2004, Innsbruck, Austria, , PP. 346-361, 2004.

[2] Anderson, D., Harvel, L., Hayes, M., Ishigors, Y., Jackson, J. and Pimentel, M., "Internet Course Delivery Making It Easier and More Effective", IEEE International Conference on Multimedia and Expo, Vol. 1. pp. 84-87, 2000

[3] Ranjit Bose, "Information Technologies for Education & Training in E-government", International Conference on Information Technology (ITCC) 5-7 April 2004, Las Vegas, USA, IEEE Computer Society, Vol. 2, pp. 203-207, 2004

[4] Schar, S.G. and Krueger, H. "Using New Learning Technologies with Multimedia", IEEE multimedia, 7(3), pp. 40-51, 2000

[5] Hayes, M. and Jamrozik, M. "Internet Distance Learning: The Problems, The Pitfalls, and The Future", Journal of VLSI Signal Processing Systems for Signal Image, and Video Technology, Vol. 29, No. 1 & 2pp.63-69, , 2001

[6] Langenbach, C. and Bodendorf, F. "The Electronic Mall: A Service Center for Distance Learning", International Journal of Electronic Commerce, 4(2):5-23, 1999

[7] Boxer, K. M. and Johnson, B. "How to Build an Online Center", Journal of Training and Development, August, 2002. http://www.highbeam.com/doc/1G1-90512522.html

[8] Consortium I.G.L "Question and Test Interoperability Specification", Stand: 24.07.2002, 2003

[9] Cisco Networking Academy Program-CAP, 2003 http://www.cisco.com/web/LA/docs/netacadmktglibrary/CiscoNetworkingAcademyLogoGuidelines

[10] Bayoumi, F., "Guidelines for Development Adaptive Mobile Learning", Second International Conference on Interactive Mobile and Computer Aided Learning (IMCL2007), Jordan, 2007

[11] Benlamri, R., Berri, J., Atif, Y., "A Framework for Ontology aware Instructional Design and Planning", International Journal of E-Learning Knowledge Society, Vol. 2, pp. 83-96, 2006

[12] IEEE STD 802.15.1 June 2002. www.ieee802.org/15/pub/TG1

[13] Douglas R. Stinson, "Cryptography theory and Practice", 3rd Edition, CRC Press, pp. 371-378, 2006

[14] J Herrera Joancomart and J. Prieto Biazquez, "A Personal Authentication Scheme Using Mobile Technology", On Proceedings of the Information Technology: Coding and Computing ITCC 2003, pp. 253-257, IEEE Computer Society 2003.

[15] W. Diffie, P.C. van Oorschot and M. J. Wiener, "Authentication and Authenticated Key Exchanges", Designs, Codes and Cryptography, 2(2):107-125, June 1992.

[16] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithm", IEEE Transactions on Information Theory, 31(4), pp. 469-472, 1985

[17] N.W. Group RFC 3161: Internet x.509 Public Key Infrastructure Time-Stamp Protocol. Internet Activities Board, 2001 http://search.yahoo.com/search;_ylt=A0oGkyQE5uNG5DcA.iZXNyoA?p=Internet+x.509+Public+Key+Infrastructure+Time-Stamp+Protocol.+Internet+Activities+Board%2C+2001+&fr=yfp-t-471

[18] A. Wouters and B. Preneel, Towards an XML Format for Time-Stamps, in Proceedings of ACM Workshop on XML, Security, pp.61-70, 2002

[19] K.M Horn and G. Martin, Authentication Protocols For mobile Network Environment Value-add Services, IEEE Transaction on Vehicular Technology, 51(2):383-392, 2002.

[20] Goh, T., and Kinshuk, "Context A ware E-learning for Multiplatform Environment – Preliminary Analysis", Proceedings of the 4th IASTED International Conference on Web-Based Education (WBE 2005), Grindelwald, Switzerland, 2005

AUTHORS

Mohammad A. AL-Fayoumi is dean of information technology faculty at Middle East University for graduate studies, Amman, Jordan (e-mail: mfayoumi99@yahoo.com)

Sattar J. Aboud is professor in the department of computer information systems/faculty of information technology at Middle East University for graduate studies, Amman, Jordan (e-mail: sattar_aboud@yahoo.com)

Mamoun S. AL Rababaa is head of information systems department at Al-al Bayt University, Amman, Jordan (e-mail**:** mam_68@yahoo.com)

Manuscript received 6 July 2007. Published as submitted by the authors.