SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC Transactions on Networks and Communications

VOLUME 2, ISSUE 4
ISSN: 2054 - 7420

Adaptable mobile user interface for securing e-learning environment

Mohanned A. aljbori, Shawkat K. Guirguis, Magda M. Madbouly
Department of Information Technology, Institute of Graduate Studies & Research, Alexandria University, Alexandria, Egypt
mohannedta@yahoo.com, Shawkat_g@yahoo.com, mmadbouly@hotmail.com

ABSTRACT

E-Learning is a pedagogy empowered by Information and Communication technologies supporting education/training. While e-Learning exists over the past decade and a half, it is do not receiving considerable attention only in the recent times. Both Industry and Academia are heavily depending on e-Learning in streamlining their teaching process, and also E-learning has provided us with the capability of providing quality education to masses without restricting them to specific time or place, So that E-Learning become the most used and popular teaching method in universities with availability of E-learning tools and techniques, development of technology communications and networks. We can say that distance education's popularity is increasing day by day and has become one of the most preferred methods for obtaining information. And it provides great facilities in many aspects according to traditional education. One of the most effective parameters in Electronic Learning or E-Learning systems' success is the security of these systems. But this feature is ignored in the most of cases. An E-Learning system has different user groups such as authors, teachers and students. Each of these groups has special and unique security requirements. In this paper we will work on secure e-learning environment against unauthorized access through design a system for securing and control access to e-learning environment in distance learning institutions by adaptable mobile user interface associated with the token code generator Technology for learners who use mobile devices to access educational content.

Keywords: E-learning, Mobile learning, E-learning problem, E-learning challenges, Adaptive Mobile user interface.

1 Introduction

Nowadays, e-learning system has becomes popular among the educational institutions. This is because E-learning system gives a lot of benefits to people such as guaranteed 24-hour response to student questions, education taking place anytime, anywhere and searchable

DOI: 10.14738/tnc.24.360
Publication Date: 24th August 2014
URL: http://dx.doi.org/10.14738/tnc.24.360

knowledge base. E-Learning is also quite effective in its ability to produce measurable results by monitoring attendance, effectiveness, performance, and recording test scores [R34], Researchers and Educators have been proposing lots of innovative designs for the development of E-Learning environments. The focus of these designs is to improve the quality of learning and provide personalization and convenience to users. Every researcher, educator believes that there should be major difference between the conventional learning and E-Learning [R35].

One of the major constraints of mobile learning is difficult to develop learning environment for mobile users, since we can't use mobile devices in the same way, we use desktop computers. Mobile devices have distinct capabilities, such as limited computing powers and small size screens. On other hand, mobile devices differ from each other by their hardware and software capabilities like computing power (processor power, memory size), screen size and resolution, operating system, web browser, script languages, file formats, etc. A number of aspects need to be dealt with before the true Potential of m-learning environment can be exploited. Some of these aspects include development of interface compatible to all kind of mobile devices [R36], Trust relationships among learners are important for collaboration activities in e-learning environments. A trust relationship may need to be developed between two unknown learners who find them working together. The meaning of trust differs from one context to another [R37]; the new strategies will reshape the role of education and create enduring advantages for both students and universities. Digital information sent from the organizers to students or agents may not be further disseminated with some commercial reasons. Therefore unauthorized dissemination of digital content has emerged as one of the most problematic and challenging issues in information security on E-Learning [R38].

E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network. E-learning (or Internet-based learning) could be seen as a professional level of education but with the advantages of lower time and cost. Some other advantages of e-learning include larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility. In a typical e-learning environment the lecturers, students and information are in different geographical locations (as depicted in Figure 2) and are connected via the Internet [R33] [R32] [R39] [R40] [R41] [R54] [R47] [R48] [R49] [R50] [R51].

There are six technical countermeasures that should be adhered to when implementing information security within any education environment. Implementing these countermeasures will help to ensure that lecturers and students as well as data (such as student marks and financial information) are properly protected against possible security incidents. These information security countermeasures are (Identification and Authentication, Authorization, Confidentiality, Integrity, Non-Repudiation, Availability) [R39] [R33] [R40] [R41] [R42] [R43] [R44] [R45] [R46] [R47] [R50] [R51].

Adaptive User Interfaces (AUIs) can provide potential benefits for addressing usability issues. Adaptation of the UI has been identified as an important aspect to be considered in the design of modern information systems. Adaptation techniques include adapting what information to present (information adaptation), how to present this information (presentation adaptation) and how to interact with this information (interface adaptation) [R53] [R52].

2 Related Work

The security Solution for E-learning Applications by using Open ID: [R10] is one of the works related to this section, this paper presents the main characteristics of Open ID standard and how this standard could be implemented for a distributed, Web-based, e-learning application, And another work by Huping Wang, Chunxiao Fan, Shuai Yang, Junwei Zou, Xiaoying in [R11] presented and describes a framework to enhance the security of OpenID with One-Time Password (OTP), In [R16] by Yu-Lin Jeng, The proposed architecture in this paper emphasizes the advantage of OpenID deployed in a decentralized environment composed of system nodes.

Secure multi agent e-Learning Applications: The related work in this section is [R2] by Carine G. Webber, Maria de Fátima W.P.Lima, Marcos E.Casa, Alexandre M.Ribeiro, in this paper presents some results in the intersection of three technological fields: e-learning, multi agent systems (MAS), and standards to improve the development of secure systems, And another work in [R19] by Shantha Visalakshi. U et al, Author Presented in this paper, proposed architecture with an enhanced security agent along with the other agents of the system, By Sadaf Ahmad, Mohammad Ubaidullah Bokhari in [R23] , proposed a new architecture for Multi agent based system for e-learning environment wherein in addition to these basic feature, the focus is interactivity and eases of use, The study presented by Umit Kocabicak Deniz Dural in [R5] it based the combining different e-learning systems that is necessary for distance education. And then, a solution is proposed to find about the security problems that occur while combining these systems, with XML web services.

Security in E-Learning system: The related work in this section is [R3] by El-Khatib, K., Korba, L., Xu, Y., and Yee, G., in this paper examines privacy and security issues associated with e-learning, Another related work presented by Jianming Yong in [R4] it proposes to use the alias and anonymity to implement the privacy preservation for e-learning systems, In addition, the work presented by Shadi R Masadeh, Nedal Turab, Farhan Obisat in [R9], in this article, he proposing a model for a secure e-learning system designed to be implemented by computer centers at universities.

Security mobile learning: The related work in this section presented by Jianming Yong in [R6], this paper systematically discusses the security and privacy concerns for e-learning systems. Five-layer architecture of e-learning system is proposed, Another related work by Ivica Boticki, Natasa Hoic-Bozic and Ivan Budiscak in [R7], This article presents a system called MILE and its extensible context-aware architecture which supports the use of mobile devices in blended learning environments.

Secure e-learning systems: The related work in this section presented by Jorge Fontenla Gonza´ lez, Manuel Caeiro Rodrı´guez, Martı´n Llamas Nistal, Luis Anido Rifon. In this paper introduce Reverse OAuth – a protocol to enable the granting of authorization to access protected resources in educational environments [R8].

Secure e-contents system for multimedia interchanges: The related workin this section in [R12] by Shadi R. Masadeh, Bilal Abul-Huda andNidal M. Turab. The main objective of this research is to build a novel multi-media security system (encrypting / decrypting system) that will enable E-learning to exchange more secured multi-media data/information.

Secure distributed e-learning and m-learning environments: The related work in this section presented by Georgios Kambourakis, Denise-Penelope N. Kontoni, Angelos Rouskas, Stefanos Gritzalis in [R13]. This paper discusses the potential application of ACs in a proposed trust model, And another related work it [R21] presented by Amjad Mahfouth. In this paper he proposes authentication techniques between universities in Avicenna Virtual Campus Project in Euro Mid Infrastructure Network.

Author’s Security in Electronic Learning: The related work in this section presented by Ali Naserasadi in [R1]. In this paper, Ali NaserAsadi has distinguished security importance in E-Learning systems from authors’ point of view, investigated security requirements and the manner of authors’ security risk analysis. Also, he suggested some approaches for educational content protection.

Securing an e-Learning Ecosystem: The related work in this section represented in [R14] presented by P.R.Lakshmi Eswari. Through this paper, various security & privacy risks associated with e-Learning are enumerated and a process framework is proposed for securing an e-Learning Ecosystem, which helps to address the security problem in a systematic way in order to foster the benefits of e-Learning.

Secure Collaborative Multimedia Learning: The related work in this section presented by Anastasia Balia, Dimitrios Koukopoulos in [R15]. In this work, present an online collaborative learning environment where the instructors insert learning material that the learners can view. User and course material classification aims at supporting distance learning scenarios that cover the needs of various user groups such as art classes, teachers and students. This learning material is essentially multimedia cultural content, distributed via the Internet and so it must be protected against any misuse, and another related work it [R20] this paper presented by Dimitrios K. Koukopoulos, Georgios D. Styliaras. This paper proposes a web-based system for organizing the creation and the interaction in multimedia web-based environments that permit the collaboration among artists, audience, curators and publishers.

Secure of Open Source Software by using Digital Signature: The related wok in this section represented in [R17] by M. Tariq Banday. This paper discusses methods for attaining authentication and integrity of Open Source Software for the purpose of its distribution.

Secure ICT environment for educational systems: The related work in this section [R18] presented by Yu-Hsiu Chuang • Chi-Yuan Chen • Tzong-ChenWu. Han-Chieh Chao. In this paper, investigate current situation of Taiwan Ministry of Education ICT security development and provide a case study. Also discussed challenges and solutions for improving ICT security environment in educational system.

WiMAX Security Issues in E-learning Systems, The related work in this section [R22] presented by Felician ALECU, Paul POCATILU, Sergiu CAPISIZU, in this paper They discussed the use of WiMAX Security Issues in E-learning Systems, the WiMAX (Worldwide Interoperability for Microwave Access) is a point-to-multipoint wireless network based on IEEE 802.16 standard. Tha WiMAX signal is broadcasted from a base station to the wide-geographically spread receivers. WiMAX enabled mobile devices [R22].

3 Proposed Methodology

3.1 Characteristics of Proposed System

Proposed our system provide access control capabilities, i.e., user authentication and authorization of user actions, as well as confidentiality and integrity of communication, Authentication is the confirmation of a principal identity with a specified or understood level of confidence. Authorization is the process of determining whether the particular entity has the right to perform some action on some resource. Authentication and authorization are the main elements of access control, which provides protection of resources against unauthorized access. Confidentiality and integrity of data transmitted over the network. Through adaptable mobile user interface associated with the token code generator Technology for learners who use mobile devices to access educational content, Fig 3.1: Shows the proposed System architecture to secure e-learning environment.

3.2 The Potential problems

In this section, will explain the potential problems that facing of mobile users, and the most important hacking cases that may be exposed to mobile users, and proposed solution for this cases:

3.2.1 Losing device:

Is one of the common problems experienced by users of mobile, In this case, the intruding on the device and try to use the real user data to access the e-learning environment, so we proposed solutions to solve this problem, First, the real user must be, logon to the e-learning environment of another device in the fastest time, This process leads to automatic logout process for the losing device, Through this process we were able to cut the way for hackers to access e-learning environment, But in the other case, if the intruder was able to access the e-learning environment Before enabling real user of a logon to the e-learning environment from another device, In this case we worked on making mobile user interfaces have the ability to adapt with the role of the client, This procedure gives us the possibility of a scalable process intruding on the e-learning environment to less space as possible and not to leave full freedom to the intruder for movement within e-learning environment.

3.2.2 Network Monitoring:

Is one of the methods used by the hacker to get a user name and password for the real user, Our solution proposed to this problem is to make the process of using username and password for the real user only once, During login for the first time only, Therefore, the access to username and password in this case are almost impossible, Even if it were to get username and password for the real user, In this case it cannot login from another device because it requires sending additional information about the real user to the server-side, Here we close the road in front of hacker again in the process of hacking the e-learning environment by this method.

3.2.3 Mobile client hacking:

This method is most commonly used by the hacker to access into the database record For the Pirate device, In the hope of getting username and password for the real user, Or trying to decode the token code to getting the username and password through which, So it was our proposal to solve this problem is to work on make the process of generating token code based on (unique device ID, current time), So we cannot use the same token code by another device, As for the decode the token code to getting a username and password from through it, So we worked on making this task impossible by making token code encrypted by one way (Hashing), and trying to get a username and password real user through the mobile client data hacking Will be a failed, Because username and password are not stored within the mobile client database record, but they are stored on the server Side only, Therefore cannot be accessed in this way and so we In this case were able to stop the hacker access into e-learning environment again.

3.2.4 The proposed technical to solve the problem:

Adaptable mobile user interfaces with the role of the mobile client and integration with Token Code technology that depend on the idea of reduce the number of times you send your username and password to the server. Therefore the Idea proposal is to generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context, and Generate token code sent to the server as an alternative for the username and password. The idea briefly is: send the username and password to the server only once (i.e. in the login process the first time), During this process the token code is generated based on the unique device ID, User ID, username, password and current time, then the token code is sent to the mobile client to be stored as a database record, then each time you request electronic content it will be sent by the token code without username and password.

3.3 System components

3.3.1 Mobile client

Also called mobile apps, it is a term used to describe Internet applications that run on smartphones and other mobile devices. Mobile applications usually help users by connecting them to Internet services more commonly accessed on desktop or notebook computers, or help them by making it easier to use the Internet on their portable devices. Basic idea behind the Client Framework is to provide services to client applications. In addition to that, its important function is the manifestation of distributed events as .NET events on the client side [R7]. Such as operating systems and browsers act as the primary client software that is using application programs of smart phones. The browsers of smart phones are used to access data in the mobile learning system server. And JavaScript to communicate between user requests and server results [R26].

3.3.2 API (web service)

APIs (Application Program Interface) in order to use the available web services. Learning resources retrieved from the web consist of text, pictures, and videos. APIs are not standard [R24]. A mediator between The Mobile Client (MC) and the Security Manager (SM), it creates a session for MC and exchanges data with the Identity Provider (IP), token code repository (TCR), UI generator, and e-learning service.

3.3.3 Identity provider (validator):

It is home institution of the User within the federation. The Identity Provider that encapsulates information about the User (e.g. authentication, profile attributes) and sends them to the Service Provider [R8]. In other words, is responsible for the registration of new users, checking the name and password of the previously registered users, and determines the role of the client.

3.3.4 User repository:

Database stores information about system’s legitimate users [R15].

3.3.5 Role repository:

It’s responsible for storing the user's role [R31].

3.3.6 UI generator:

It’s responsible for generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context [R27] [R28].

3.3.7 Token code generation:

it’s Responsible for generating the token code For each client after the login process and it is stored in the token code repository, this code is sent to the client, Through which the client can have access to the educational content, Each client keeps his own code, which is the second phase of the authentication process to access educational content. Do not change this code unless it is through a request from the client after each new login process from the same device or another one and can be changed after it expires which is determined in previously, but after the client is notified and has agreed to changing the code.

3.3.8 Token code repository:

it’s responsible for the storage token Code for each Existing user and the new ones.

3.3.9 Learning service:

It provides the possibility to host the digital educational resources, which can be accessed by the lecturer and all students either locally, or throughout the Internet. Additionally, all students, as well as the lecturer over the Internet can access the Server Platform to collect, or download the data that needs to be computed in an e-learning environment [R25]. The System database stores the basic information of students and teachers. It further contains the processing information of students learning and faculty member‘s teaching. The learning resource database consists of mobile learning courseware, electronic lesson plans, e-books, dictionaries and other mobile learning software [R26]. Briefly responsible for the educational content storage, this is an essential component in each e-Learning System.

3.3.10 JavaScript Object Notation (JSON):

It is an open standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs. It is used primarily to transmit data between a server and web application, as an alternative to XML. Although originally derived from the JavaScript scripting language, JSON is a language-independent data format, and code for parsing and generating JSON data is readily available in a large variety of programming languages. Is designed to be a data exchange language which is human readable and easy for computers to parse and use. JSON is directly supported inside JavaScript and is best suited for JavaScript applications; thus providing significant performance gains over XML, which requires extra libraries to retrieve data from Document Object Model (DOM) objects [R29] [R30].

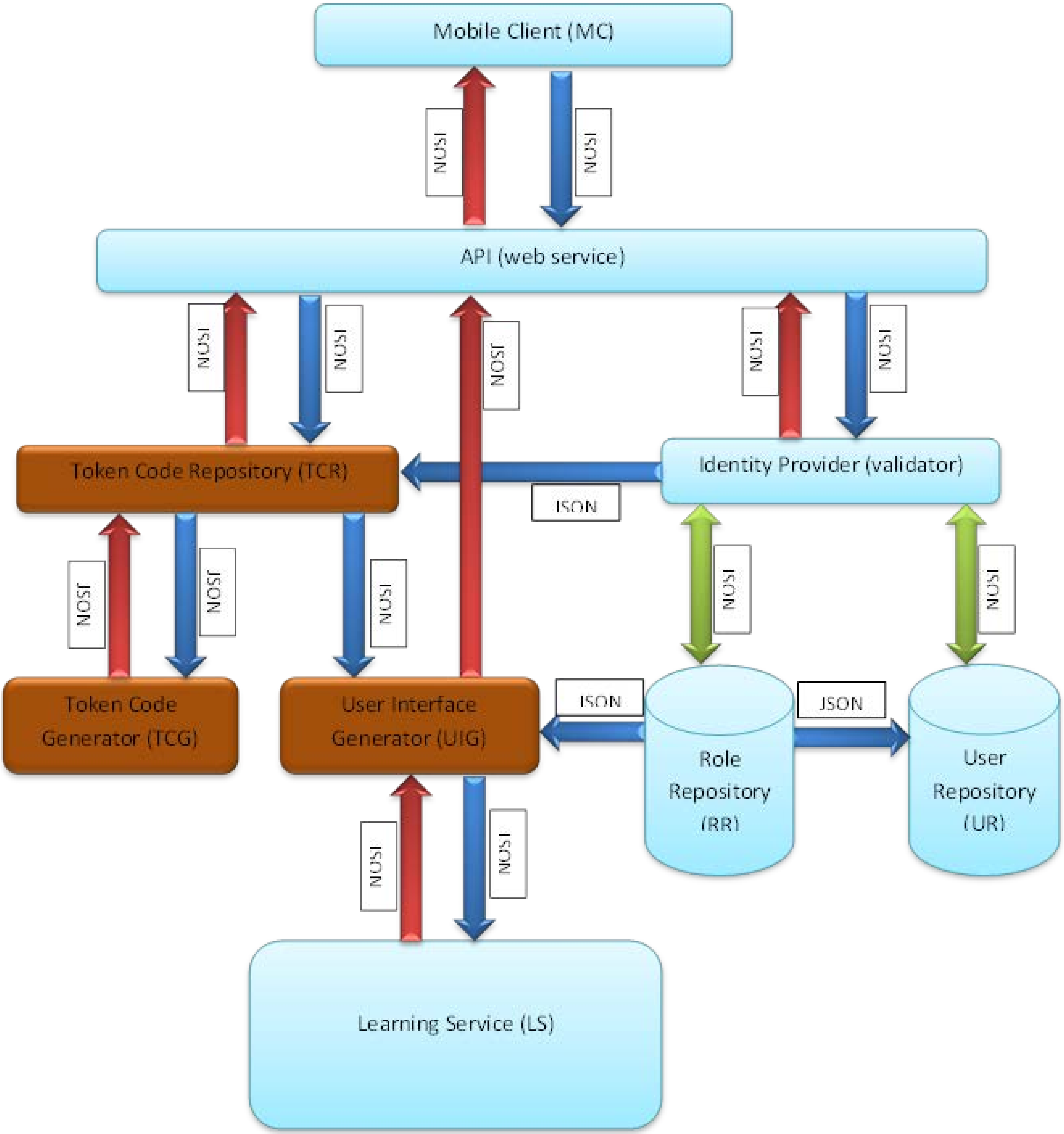


Figure 1: The proposed System architecture to secure e-learning environment

3.4 Data flow in system architecture:

There are three scenarios for the data flow in the system; the first scenario begins the process of recording data of the user who wishes to register in the system. The second scenarios are the process login to the system by the user for the first time and request the electronic content. And ending system processes by the third scenario Special Process of electronic content request through the proposed technology for the protection of educational content in which it operates technology adaptable mobile user interfaces Enhanced by token Code technology. These three scenarios will be explained below.

3.4.1 The registration request case:

1. Mobile client (MC) sends the registration request to the (API).
2. The (API) send the registration request to the identity provider (validator).
3. The (validator) verification of registration information, If information previously registered then returns an error message in the registration process, If the information is not previously registered then complete the registration process by store the user information in user repository (UR) and role repository (RR) and return message to complete this process.

3.4.2 The Login and educational content request case:

1. Mobile client (MC) sends Login and learning service request to the (API).
2. The (API) send request to the (validator).
3. The (validator) Verifies the customer's identity by check information in (UR) and (RR), If the client is not registered, then Return the message refuse to accept login request, If the client is registered, then request is accepted and send a request to token code repository(TCR) for verification of the token code.
4. (TCR) Verifies from the token code, if it was token code for this client, then going directly to the Seventh step, if it was not token code for this client, then (TCR) send request to the token code generator (TCG) to generate token code.
5. The (TCG) generate token code and send it to (TCR).
6. The (TCR) store the token code and sent it to the (API) and the (API) send the token code to the (MC), In addition, the (TCR) send a request to user interface generator (UIG) to generate user interface.
7. The (UIG) generate user interface fit with the role of the client and the type of content requested, and send request to learning service (LS) for the purpose of sending educational content.
8. The (LS) send educational content to the (UIG).
9. The (UIG) send user interface and educational content to the (API).
10. The (API) send this content to the (MC).

3.4.3 The educational content request by adaptive mobile user interface and token code case:

1. The (MC) send educational content request by the token code to the (API).
2. The (API) send this request to the (TCR).

3. The (TCR) Verifies from the token code, if the token code was not correct then Return refused for accept the request message, if the token code was correct then (TCR) send educational content request to the (UIG).
4. The (UIG) generate user interface was fit with the role of the client and the type of content requested, and send request to learning service (LS) for the purpose of sending educational content.
5. The (LS) send educational content to the (UIG).
6. The (UIG) send user interface and educational content to the (API).
7. The (API) send this content to the (MC).

4 Experiments and Results

4.1 Research Material

4.1.1 Used tools:

The proposed system described in chapter 3 has been tested by using (Advanced REST client for Google Chrome) this tool it web developer's helper program to create and test custom HTTP requests. Have many advantages, but will mention some of the features that concerns us in our research (Integrated with Google Drive, Debug socket (via web socket API), JSON response viewer, XML response viewer, In addition, we used (Bulk URL Opener Extension): This tool used in Open multiple URLs at once; Bulk URL Opener Extension just lets our open multiple URLs at once (in new tabs or windows) And we used HashKiller.co.uk allows you to input an MD5 hash and search for its decrypted state in our database, basically, it's a MD5 cracker / decryption tool.

4.1.2 Used Device:

The algorithm, presented in this thesis, is implemented with a laptop HP model with the following specifications of Intel Core i7 3612QM 2.1 GHz with 4GB RAM, Video Graphics ,ATI HD 7670 Video Memory 1GB of Turbo-Cache™ video Memory including 3021 MB dedicated video memory and Display 15.6 LED High Definition Bright View Widescreen (1366 x 768). This machine is equipped with operating system Windows 7 Home Basic.

4.1.3 Used Software:

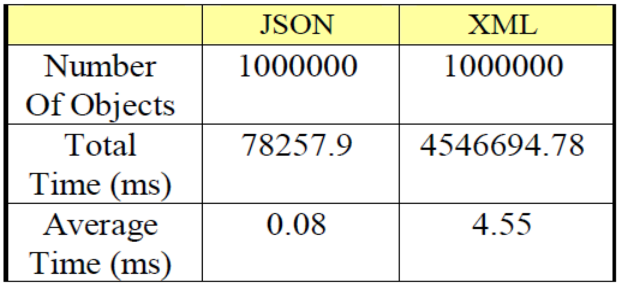
The proposed image watermarking scheme has been implemented using Firstly, JavaScript (JS): is a dynamic computer programming language. It is most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. It is also being used in server-side programming, game development and the creation of desktop and mobile applications, Secondly, PHP: is a server-side scripting language designed for web development but also used as a general-purpose programming language. Originally created by (Rasmus Lerdorf) in 1995, the reference implementation of PHP is now produced by The PHP Group. PHP code is interpreted by a web server with a PHP processor module, which generates the resulting web page: PHP commands can be embedded directly into an HTML source document rather than calling an external file to process data. It has also evolved to include a command-line interface capability and can be used in standalone graphical applications, Thirdly, JSON or JavaScript Object Notation: is an open standard formatting that uses human-readable text to transmit data objects consisting of attribute–value pairs. It is used primarily to transmit data between a server and web application, as an alternative to XML.

4.2 Research Results:

4.2.1 First experiment:

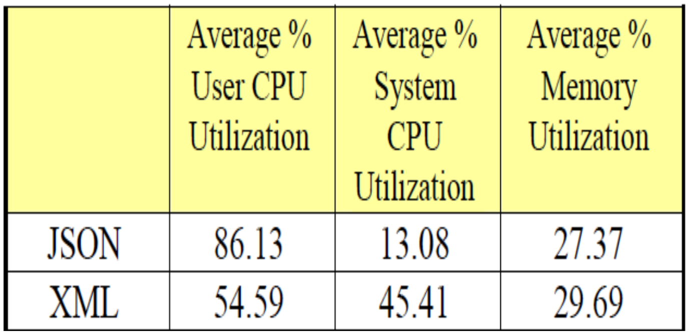
In the first experiment, (Results illustrate the differences between JSON and XML encoding under varying transmission scenarios. This section presents the metrics obtained for the average measurements, compares the metrics of transmitting high versus low number of encoded objects, and determines whether JSON and XML are statistically different for each of our measurements. We present both scenarios' measurements and discuss their implications) [R29] in this Scenario is a time-consuming transmission of a large quantity of objects. Large numbers of objects are used in order to achieve accurate average measurements. The client sends one million encoded objects to the server for both JSON and XML. We measure timing and resource utilizations. Table 1 and table 2 list the measurements and respective values obtained from this trial [R29].

Table 1: JSON vs. XML Timing [R29]



	JSON	XML
Number Of Objects	1000000	1000000
Total Time (ms)	78257.9	4546694.78
Average Time (ms)	0.08	4.55

Table 2: JSON vs. XML CPU/Memory [R29]



	Average % User CPU Utilization	Average % System CPU Utilization	Average % Memory Utilization
JSON	86.13	13.08	27.37
XML	54.59	45.41	29.69

4.2.2 Second experiment:

In this test, we compared the difference results between the processes of login to e-learning environment from client side to server side, By using the token code once and by (user name, password) again, We did this test in the case of synchronization login to e-learning environment, We used the number of samples begin ten login process and then gradually increasing to sixty login process and we got the results shown in the table 3 and Figure 2.

Table 3: Different login time by using token code & (username and password)

number of login process	Average login time by token cod (MS)	Average login time by username & password (MS)
10	9.85	26.2
20	11.3	28.34
30	13.7	30.17
40	15.65	32.45
50	17.23	34.66

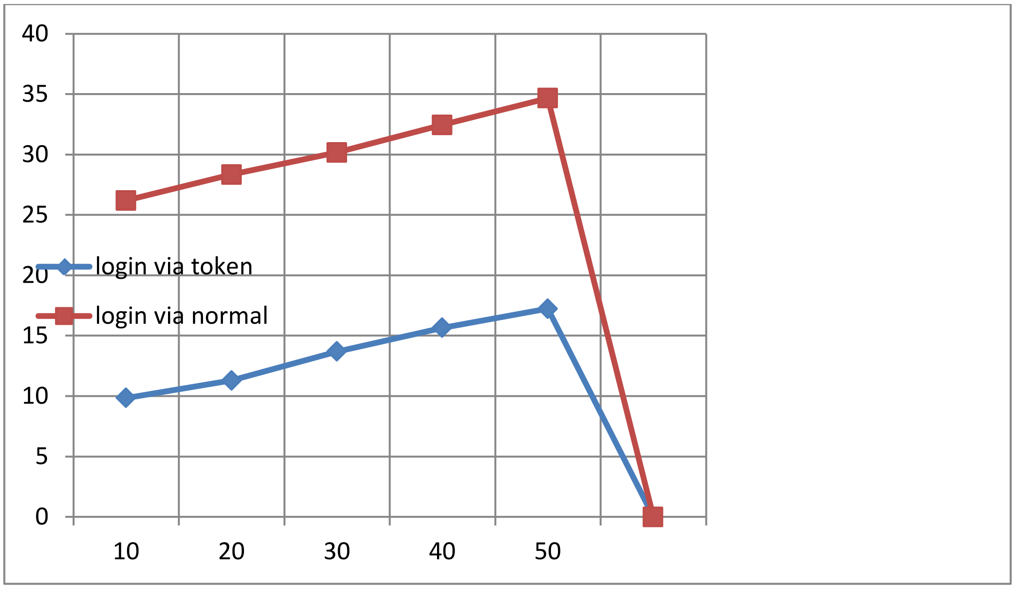


Figure 2: different login time by using token code & (username and password)

4.2.3 Third excrement:

In this test, we compared the difference results between the processes of getting the e-learning content from client side to server side, By using the token code once and by (user name, password) again, We did this test in the case of synchronization to get the e-learning content, We used the number of samples begin ten users and then gradually increasing to sixty user and we got the results shown in the table 4 and Figure 3.

Table 4: different result to getting e-learning content by using token code & (username and password) in synchronization case

synchronization		
No. of users	Average Getting time via token by (S)	Average Getting time via normal(S)
10	0.66	0.74
20	1.15	1.39
30	2.25	2.71
40	3.2	3.37
50	4.36	4.81
60	5.4	5.86

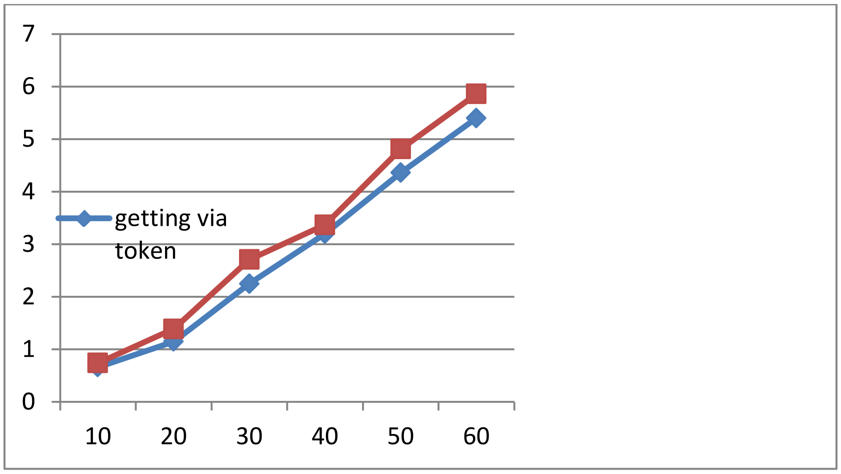


Figure 3: different result to getting e-learning content by using token code & (username and password) in synchronization case

4.2.4 Fourth experiment:

In this test, we compared the difference results between the processes of getting the e-learning content from server side to client side, By using the token code once and by user name and password again, We did this test in the case of (A synchronization) to get the e-learning content, We used in our test this ten users asynchronously where are not dealing with the second user until the completion of the first user, as well as order until the completion of all subscribed users and we got the results shown in the table 5 and Figure 4.

Table 5: different result to getting e-learning content by using token code & (username and password) in (A synchronization) case

A synchronization		
No. of users	Getting time via token by(MS)	Getting time via normal(MS)
1	17.44	21.14
2	17.56	21.27
3	17.61	22.85
4	19.15	23.45
5	19.23	23.92
6	20.36	24.26
7	20.42	24.78
8	21.17	25.11
10	21.28	25.65

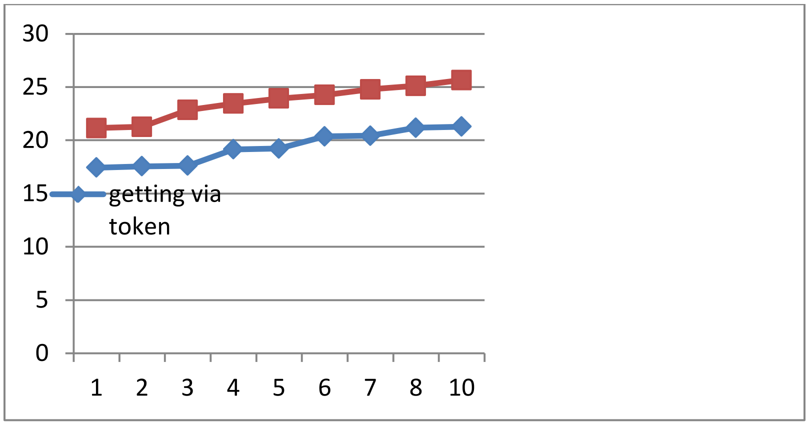
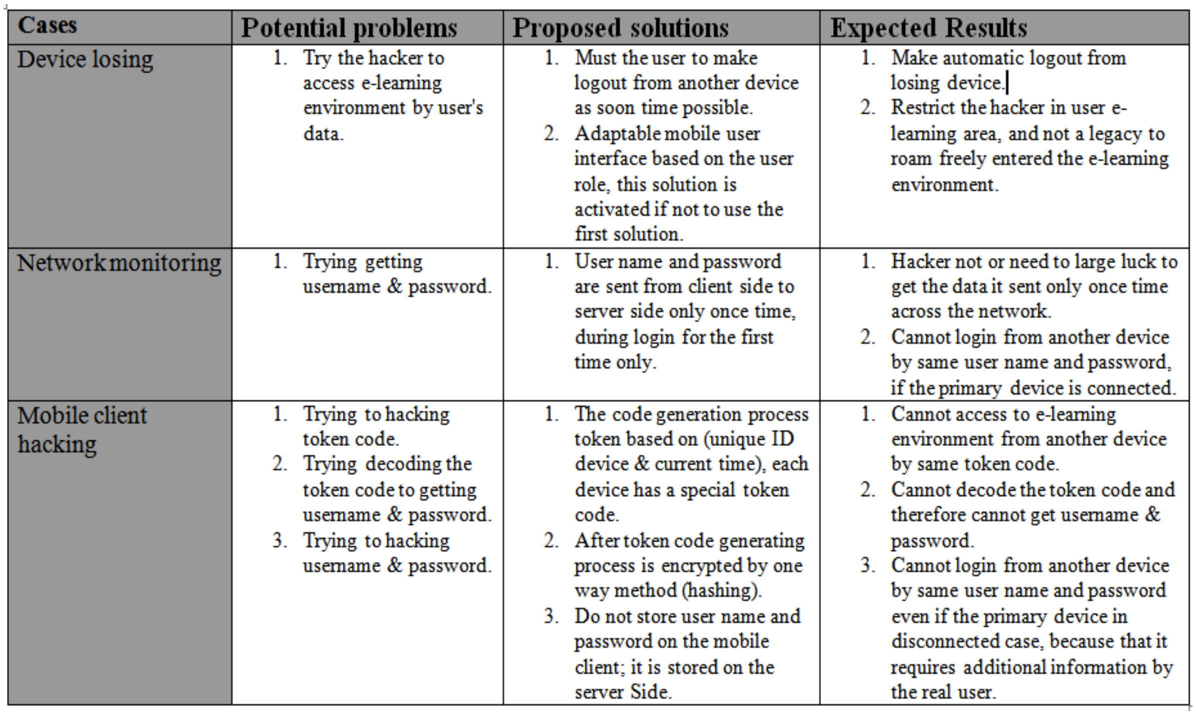


Figure 4: different result to getting e-learning content by using token code & (username and password) in (Asynchronization) case

4.2.5 Other experiment:

In this experimentation, we put summary table shows the proposed solutions to the problems faced by mobile users secure environment for e-learning and the results of these solutions.

Table 6: Potential problems, solution and the results



Cases	Potential problems	Proposed solutions	Expected Results
Device losing	1. Try the hacker to access e-learning environment by user's data.	1. Must the user to make logout from another device as soon time possible. 2. Adaptable mobile user interface based on the user role, this solution is activated if not to use the first solution.	1. Make automatic logout from losing device. 2. Restrict the hacker in user e-learning area, and not a legacy to roam freely entered the e-learning environment.
Network monitoring	1. Trying getting username & password.	1. User name and password are sent from client side to server side only once time, during login for the first time only.	1. Hacker not or need to large luck to get the data it sent only once time across the network. 2. Cannot login from another device by same user name and password, if the primary device is connected.
Mobile client hacking	1. Trying to hacking token code. 2. Trying decoding the token code to getting username & password. 3. Trying to hacking username & password.	1. The code generation process token based on (unique ID device & current time), each device has a special token code. 2. After token code generating process is encrypted by one way method (hashing). 3. Do not store user name and password on the mobile client; it is stored on the server Side.	1. Cannot access to e-learning environment from another device by same token code. 2. Cannot decode the token code and therefore cannot get username & password. 3. Cannot login from another device by same user name and password even if the primary device in disconnected case, because that it requires additional information by the real user.

5 Conclusion and future work

In our research we have proposed new method To protect e-learning environment, Through the use of adaptable mobile user interfaces and Token Code technology, We used this method rather than of traditional method which is based on (User name & password) to get the electronic content from e-learning environment, A summary of our proposal based on: Adaptable mobile user interfaces with the role of the mobile client and integration with Token Code technology that depend on the idea of reduce the number of times you send your username and password to the server. Therefore the Idea proposal is to generating user interface appropriate with the role of the client and the type of content requested, and sending requests to the learning service. Means responsible for generating user interfaces for applications, adapted to a particular user, the currently used access device and the current context, and Generate token code sent to the server as an alternative for the username and password. The idea briefly is: send the username and password to the server only once (i.e. in the login process the first time), During this process the token code is generated based on the unique device ID, User ID, username, password and current time, then the token code is sent to the mobile client to be stored as a database record, then each time you request electronic content it will be sent by the token code without username and password.

Adaptive User Interfaces (AUIs) can provide potential benefits for addressing usability issues. Adaptation of the UI has been identified as an important aspect to be considered in the design of modern information systems. Adaptation techniques include adapting what information to present (information adaptation), how to present this information (presentation adaptation) and how to interact with this information (interface adaptation), and from our view we think that adaptation of mobile user interfaces will have a major role in supporting the security system for e-learning environment.

Therefore, adaptively makes it possible for a system to behave in a different way for different users. In order to achieve that feature, adaptive systems need a user model which holds information about individual users. There are two types of Inputs when collecting data about users when creating a user model (Requesting direct input from users “explicitly” and Observing user's interaction with the system and automatically collecting information “implicitly”).

In addition, the learner needs can be classified as follows (User Knowledge, User's Interests, User's Goals and Tasks, User's Background, Individual Traits, Context of Work).

All of these things can take into consideration in future works, And use them as tools to develop the concept of adaptable mobile user interfaces, That will depend upon the security system for e-learning environment in the future.

REFERENCES

[1]. Ali Naserasadi, “Author’s Security in Electronic Learning Systems”, International Journal of Computer Applications, Vol. 21, Issue 10, pp. 25-29, 2011.

[2]. Carine G. Webber, Maria de Fátima W.P.Lima, Marcos E.Casa, Alexandre M.Ribeiro, “Towards Secure e-Learning Applications: a Multi agent Platform”, Journal Of Software, Vol. 2, Issue 1, pp. 60-69, 2007.

[3]. El-Khatib, K., Korba, L., Xu, Y., and Yee, G., "Privacy and Security in E-Learning", International Journal of Distance Education Technologies (IJDET), Vol. 1, No. 4, pp. 1-19, 2003.

[4]. Jianming Yong, “Enhancing the Privacy of e-Learning Systems with Alias and Anonymity", International Conference on Computer Supported Cooperative Work in Design, pp. 534-544, 2008.

[5]. Umit Kocabicak, Deniz Dural, “Secure and Interoperable e-Learning Platforms Based on Web Services ", International Conference on New Horizons in Education, pp. 1265 – 1271, June 2012.

[6]. Jianming Yong, "Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes“, Journalz ofUniversal Computer Science (J.UCS), Vol. 17, No. 2, pp. 296-310, 2011.

[7]. Ivica Boticki, Natasa Hoic-Bozic, Ivan Budiscak, " A System Architecture for a Context-aware Blended Mobile Learning Environment", Journal of Computing and Information Technology(CIT), Vol. 17, No. 2, pp. 165–175, 2009.

[8]. Jorge Fontenla Gonza´ lez, Manuel Caeiro Rodrı´guez, Martı´n Llamas Nistal, and Luis Anido Rifo´n, “Reverse Oath: A solution to achieve delegated authorizations in single sign-on e-learning systems”, computers & security, Vol. 28, No 8, pp. 843-656, 2009.

[9]. Shadi R Masadeh, Nedal Turab, Farhan Obisat, “A secure model for building e-learning systems”, Network Security, Vol. 2012, No 1, pp. 17–20, 2012.

[10]. Felician Alecu, Paul Pocatilu, George Stoica, Cristian Ciurea, Sergiu Capisizu, “OpenID, a Single Sign-On Solution for E-learning Applications “,Journal of Mobile, Embedded and Distributed Systems(JMEDS), Vol. 3, No. 3, pp. 136-141, 2011.

[11]. Huping Wang, Chunxiao Fan, Shuai Yang, Junwei Zou, Xiaoying Zhang, “A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP) “,Wireless Communications, Networking and Mobile Computing (WiCOM), 7th International Conference on, 2011.

[12]. Shadi R. Masadeh,Bilal Abul-Huda andNidal M. Turab, “a novel secure e-contents system for multimedia interchange workflows in e-learning environment”, International Journal of Computer Networks & Communications (IJCNC), Vol. 15, No 5, pp. 131–139, 2013.

[13]. Georgios Kambourakis, Denise-Penelope N. Kontoni, Angelos Rouskas, and Stefanos Gritzalis, “A PKI approach for deploying modern secure distributed e-learning and m-learning environments “,Computers & Education, Vol. 48, No. 1, pp. 1–16, August 2007.

[14]. P.R.Lakshmi Eswari, “A Process Framework for Securing an e-Learning Ecosystem “, 6th international conference on internet technology and secured transaction, pp. 403 - 407, Abu Dhabi, United Arab Emirates, 11-14, December 2011.

[15]. Anastasia Balia, and Dimitrios Koukopoulos, “A Secure Collaborative Multimedia Learning Scheme in Cultural Environments “,international conference on Information, Intelligence, Systems and Applications (IISA), pp. 1-5, Piraeus, 10-12 July 2013.

[16]. Yu-Lin Jeng, “An OpenID Based Authentication Mechanism in a Distributed System Environment”, International Journal of Computer and Communication Engineering, Vol. 1, No. 3, pp. 250-252, September 2012.

[17]. M. Tariq Banday, " Ensuring Authentication and Integrity of Open Source Software using Digital Signature”, International Journal of Computer Applications, IJCA Special Issue on Network Security and Cryptography NSC, Vol. 4, No. 2, pp. 11-14, 2011.

[18]. Yu-Hsiu Chuang, Chi-Yuan Chen, Tzong-ChenWu, and Han-Chieh Chao,” Establish a secure and trustworthy ICT environment for educational systems: a case study “,Journal of Intelligent Manufacturing, Vol. 23, Issue 4, pp. 965-975, August 2012.

[19]. Shantha Visalakshi. U and Shyamala. K, “Multi-agent coordination in distributed e-learning environment providing access permissions “, International Journal of Engineering and Technology (IJET), Vol. 5, No. 2, pp. 1306-1310, May 2013.

[20]. Dimitrios K. Koukopoulos, and Georgios D. Styliaras," Security in Collaborative Multimedia Web-based Art Projects", Journal Of Multimedia, Vol. 5, No. 5, pp. 404-416, October 2010.

[21]. Amjad Mahfouth, "The Authentication Techniques in Distributed E-Learning between Universities in Avicenna Virtual Campus Network", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 3, No 2, pp. 418- 422, May 2012.

[22]. Felician ALECU, Paul POCATILU and Sergiu CAPISIZU, " WiMAX Security Issues in E-learning Systems", Journal of Mobile, Embedded and Distributed Systems(JMEDS), Vol. 2, No. 1, pp. 15-20, 2010.

[23]. Sadaf Ahmad and Mohammad Ubaidullah Bokhari, “A New Approach to Multi Agent Based Architecture for Secure and Effective E-learning “,International Journal of Computer Applications(IJCA), Vol. 46, No22, pp. 26-29, May 2012.

[24]. Mohammed Alzaabi, Jawad Berri and Mohamed Jamal Zemerly, “Web-based Architecture for Mobile Learning “,International Journal for Infonomics (IJI), Vol. 3, Issue. 1, pp. 207-216, March 2010.

[25]. MD. Anwar Hossain Masud and Xiaodi Huang, “M-learning Architecture for Cloud-based Higher Education System of Bangladesh “, Mobile Computing, Vol. 2, Issue. 4, pp. 84-94, November 2013.

[26]. T. Altameem, "Contextual Mobile Learning System for Saudi Arabian Universities ", International Journal of Computer Applications, Vol. 21, No 4, pp-21-26, May 2011.

[27]. Krzysztof Walczak, Jacek Chmielewski, Wojciech Wiza, Dariusz Rumiński and Grzegorz Skibiński, "Adaptable mobile user interfaces for e-learning repositories ", IADIS International Conference on Mobile Learning, 2011.

[28]. Krzysztof Walczak, Wojciech Wiza, Dariusz Rumiński, Jacek Chmielewski and Adam Wójtowicz, “Adaptable User Interfaces for Web 2.0 Educational Resources ", IT Tools in Management and Education-Selected Problems, pp. 104-124, 2011.

[29]. N. Nurseitov, M. Paulson, R. Reynolds, and C. Izurieta, "Comparison of JSON and XML Data Interchange Formats: A Case Study", in Proc. CAINE, 2009, pp.157-162.

[30]. Antonio Sarasa-Cabezuelo and José-Luis Sierra, "Grammar-Driven Development of JSON Processing Applications", Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 1545 – 1552, 8-11 Sept. 2013.

[31]. Adam Wójtowicz, Jakub Flotyński, Dariusz Rumiński, and Krzysztof Walczak, “Securing Learning Services Accessible with Adaptable User Interfaces", Information Systems Architecture and Technology, Service Oriented Networked Systems, pp. 109-118, 2011.

[32]. Georgios Kambourakis, " Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art”, International Journal of u- and e- Service, Science and Technology, Vol. 6, No. 3, pp. 67-84, June, 2013.

[33]. Roberto G´omez C´ardenas and Erika Mata S´anchez, “Security Challenges of Distributed e-Learning Systems “, 5th International School and Symposium, ISSADS, Volume 3563, pp. 538-544, Guadalajara, Mexico, January 24-28, 2005.

[34]. Zainal Fikri Zamzuri, Mazani Manaf, Adnan Ahmad, and Yuzaimi Yunus, "Computer Security Threats towards the E-Learning System Assets”, Second International Conference, ICSECS, Volume 180, pp. 335-345, June 27-29, Kuantan, Pahang, Malaysia 2011.

[35]. Alok Tripathi, and Abhinav Mishra, "A Web-based E-Learning Environment for Information Security", International Journal of Computer Applications (IJCA), Vol. 45, No. 4, pp. 50- 54, May 2012.

[36]. Rajesh Wadhvani, and Devshri Roy, "Developing Agent Oriented Mobile Learning System ", International Journal of Computer Science and Information Security (IJCSIS),, Vol. 10, No. 4, PP. 93-98, April 2012.

[37]. Mohd Anwar and Jim Greer, “Facilitating Trust in Privacy-Preserving E-Learning Environments”, IEEE Transactions on Learning Technologies, Vol. 5, No. 1, pp. 62-73, January -March 2012.

[38]. Lili Sun, Hua Wang, and Yan Li, "Protecting Disseminative Information in E-Learning ", 6th International Conference Advances in Web Based Learning (ICWL), pp. 554–565, UK, August 15-17, 2008.

[39]. E. Kritzinger, “Information Security in an E-learning Environment “, IFIP International Federation for Information Processing, Volume 210, pp. 345-349, August 21–24, Chile 2006.

[40]. Miguel, J., Caballe, S. and Prieto, J, “Information Security in Support for Mobile Collaborative Learning “, Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, pp. 379- 384, 3-5 July Taichung 2013.

[41]. Najwa Hayaati Mohd Alwi and Ip-Shing Fan, " E-Learning and Information Security Management", International Journal of Digital Society (IJDS), Vol. 1, Issue. 2, pp. 148-156, June 2010.

[42]. Ateeq Ahmad and Mohammed Ahmed Elhossiny," E-Learning and Security Threats ", (IJCSNS) International Journal of Computer Science and Network Security, Vol. 12, No. 4, pp. 15-18, April 2012.

[43]. Vladimir I. Zuev, "E-Learning Security Models", (JMIS) Journal of Management Information Systems, Vol. 7, No. 2, pp. 024-028 April 2012.

[44]. Im Y. Jung and Heon Y. Yeom, "Enhanced Security for Online Exams Using Group Cryptography ", IEEE Transactions on Education, Vol. 52, No. 3, pp. 340-349, August 2009.

[45]. Defta (Ciobanu) Costinela – Luminita, "Information security in E-learning Platforms ",3rd World Conference on Educational Sciences, Volume 15, pp. 2689–2693, Istanbul, Turkey 2011.

[46]. Professor Aurel ŞERB PhD, Lecturer Costinela - Luminiţa DEFTA, PhD. Candidate, Junior Lecturer Nicoleta Magdalena IACOB, PhD and Lecturer Marius Cristian APETREI, PhD. candidate, "Information Security Management In E-Learning ",Knowledge horizons Journal , Vo. 5, No. 2, pp. 1 - 6, 2013.

[47]. Nikhilesh Barik and Dr. Sunil Karforma, "Risks and Remedies In E-Learning System", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, pp. 51-59, January 2012.

[48]. S.Hameetha Begum, T.Sheeba and S.N.Nisha Rani, "Security in Cloud based E-Learning ",International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1,, pp. 270-278, January 2013.

[49]. Mr. Dhiraj K. Chandak and Prof.Mr. M.M. Bartere, "Security in Cloud Based M-learning", International Journal of Computer Science and Management Research, Vol. 2 Issue 4, pp. 2163-2170 , April 2013.

[50]. Defta (Ciobanu) Costinela – Luminita, "Security issues in e-learning platforms ", World Journal on Educational Technology, Vol. 3, issue. 3, pp. 153-167, December 2011.

[51]. Maria Nickolova and Eugene Nickolov, "Threat Model for User Security in E-Learning Systems", International Journal "Information Technologies and Knowledge, Vol. 1, No. 1, pp. 341-347, 2007.

[52]. Kyle Montague, Vicki L. Hanson, and Andy Cobley, "Adaptive Interfaces: A Little Learning is a Dangerous Thing ", 6th International Conference Universal Access in Human-Computer Interaction. Design for All and eInclusion (UAHCI), Volume 6765, Orlando, FL, USA, pp. 391–399, July 9-14, 2011.

[53]. Janet L. Wesson, Akash Singh, and Bradley van Tonder ", Can Adaptive Interfaces Improve the Usability of Mobile Applications, Second IFIP International Federation for Information Processing, pp.198–187 , Australia, September 20-23, 2010.

[54]. E. Kritzinger, and S.H von Solms, " E-learning: Incorporating Information Security Governance", Issues in Informing Science and Information Technology, Vol. 3, pp. 319-325, 2006.