A TOTAL SECURITY MODEL FOR E-EDUCATION;

* Khader M. Titi , ** Saad Al-Aani , *** Riyadh Al-Shalabi

* Arab Academy for Banking & Financial Sciences - Amman - Jordan
e-mail: rshalabi@aabfs.org

** Al-Ahliyyah Ammanuniversity Amman - Jordan
e-mail: saadal-ani@ammanu.edu.jo

*** Arab Academy for Banking & Financial Sciences - Amman - Jordan
e-mail: ktiti@ammanu.edu.jo

ABSTRACT

Nowadays, new information and communication technologies have become major resources and basis for learning in higher education. Technologies have several potentials to support different instructional strategies and provide an efficient way of delivering electronic course material and improving comprehension. The contemporary universities need to increase lifelong learning opportunities to its students any time, any place and at any rate to be successful in the global learning marketplace [1].

The use of e-leaning in the learning process has grown significantly in the last few years, however, it is a relatively insecure, hence, most learning organization haven't yet taken into considerations any new strategy for securing e-learning process [2]*. Additionally, implementing e-learning is complex. Implementing e-learning is about project management, change management and risk and security management* [3].

The main aim of this research is to provide a new mechanism to protect the e-learning material from unauthorized distribution, to protect the e-course material from being altered or modified from any intruders and to provide new tools, strategies and mechanism to make the e-learning process more secure and trustee.

Key words: *Security, e-learning, Encryption*.

1. INTRODUCTION

The topic e-learning is having much attention especially because world-class universities such as MIT, Harvard and Stanford in the United States and Oxford in the United Kingdom are implementing it [4]. E-learning can be defined as the online delivery of information for purposes of learning, training and knowledge management [5]. This definition means that the Internet and computer will be used in the e-learning process. Thus, e-learning is more complex and intertwined the opportunities for intrusion and attack. E-learning security involves more that just preventing and responding to cyber attacks and intrusion. It involves copyright protection, integrity, availability, non-repudiation, authentication and authorization.

Using the Internet in the learning process is very beneficial to both students and learning institutions.

The core reason why Internet is gaining so much interest lies on its ability of joining and interoperating heterogeneous communities. A lot of users who use different platform with different computer hardware and different computer software can communicate and interactive with each other easily on the Internet. The Internet and its potential and capabilities are very attractive, however, the current standards behind the technology need to be justified very carefully, before deploying the Internet for very sensitive applications such as e-learning system. Since, default Internet transactions are unencrypted and unsecured, and they can establish the potential for disaster and failure [6].

Computer security is the shield that all types of organizations and governments use to protect sensitive, commercial and classified information from unauthorized users and from malicious attacks. A break of this shield has implications that go far beyond any financial form that could be assigned to such an intrusion or adversary. The concepts of computer security are practically basic in nature, however, implementing security in a continually changing technological environment is a big challenge, but it has to be met by organizations, individual users and governments.

Hackers intent on personal financial gain are the most rapidly growing threat to organizations and users [7]. Users are finding that breaking into companies can be very profitable - either selling information obtained, or using the compromised system for their own benefit.

Organizations such as learning institutions that want to implement an e-learning system must protect all its resources such as: electronic learning material, students' private information, transaction processing and other types of data on transit.

In this research a number of security issues in the delivery of e-learning course materials and copyrights protections will be research and proposes a number of solutions to tackle these issues. Through this, the researcher hope to highlight typical security requirements in e-learning systems and will give a brief description of the application and identify a number of essential security issues for the safe operation of the system and a number of techniques, including those to ensure Web server security, cryptographic means and implementation guidelines, are considered and employed for meeting the security requirements of the system.

2. SECURITY ISSUES OF E-LEARNING

As pointed out by Furnell [8], little attention and small concentration has been devoted to the security concerns of e-Learning. E-Learning institutions have to present innovative approaches in its e-learning process. Effective adoption of e-learning system has to be comprehensive and should be safe-enough privacy and security for delivery and collaborative learning.

Most of all, security issues cover all security problems connected to network especially the Internet technology. These security issues encompass of denial of service for e-learning systems, integrity of data delivery, copyright protection and unauthorized access to the private resource or information in the e-learning systems. Copyright protection prevent student from downloading the e-Course of the course material and view it offline. Thus, method and approaches have to be presented to let student view the content offline at the same time these content have to be well protected from copyright violation. It is, therefore, a great privilege for an e-Learning system to permit its students to download the e-Course material onto their own computers and view it offline. This will let students study the material anytime, anywhere, even when they are not connected to the Internet. But, Caution must be considered to prevent users from making illegal copies of the downloaded materials.

According to Mcleod and Schell [9] security targets are to be derived by examining the three aspects of data security. These aspects are:

- **integrity**, providing an accurate representation of the physical system they represent; data can be altered or deleted while it is in transit or after it stored.
- **availability**, for those authorized to use it;
- **confidentiality**, protecting data and information from disclosure to unauthorized persons.

However, there are other issues related to security such as:

- **Intrusion**

Unauthorized intruders can expose a corporate system. They tackle the system by collecting significant information concerning a target network, scanning a target network in order to identify and understand the system, and identifying valid user account, poorly protected resource, and vulnerability of the system [10] .

As Baker [11] said “information security is a people crisis”. According to a number of executive managers, they viewed that 81.60 % of security threats come from their employees [11]. Normally, a majority of employees are lack of information and awareness regarding security issues. Therefore, these borders appear to be vulnerable for unauthorized intruder to get the significant information or permission. For instance, some employees may:

○ choose simple password which is easy to guess by intruders such as birthday or some special events names;

○ write down their password on a piece of paper and posting it on their VDU;

○ download unknown file or email which may be infected with virus, worms or Trojans.

- **System Vulnerable**

Usually, the system may have some vulnerability. This is common problem for new hardware and software because, usually, a number of vulnerability could be exposed after launched the system. For instance, for IIS 3.0 server, there is a significant vulnerability, ASP Dot Bug, which attacker can easily view ASP source code by adding dots to the end of ASP URL [10].

- **Denial Of Service**

The idea of a denial of service attack is to prevent the company from using own resources [12] and to prevent legitimate users from accessing recourses they need from the system. For instance, since corporate server was down resulted by denial of service attack, the organization’s clients would find an error page when they access to the organization’s Website. As a consequence, the organization might have problems such as losing clients, wasting time, having reputation problem especially if the organization performs business related to security.

2.1 RSA, HASH FUNCTION AND DIGITAL SIGNATURES

The RSA cryptosystem is a public-key cryptosystem that presents both encryption and digital signatures. Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA system in 1977 [13]. RSA stands for the first letter in each of its discoverers’ last names [14].

A digital signature is an identifier, which could be used to authenticate the sender of an electronic message or document. This approach could also be used to guarantee the integrity of the message or document that no modifications have been made since it was signed as well as to date/time-stamp the document at signing. Additionally, the signatory cannot repudiate or refuse to acknowledge his digital signature, nor can the document be easily faked.

The digital signature uses cryptographic tools to create an electronic identifier, however it can be used with any message, whether the message is encrypted or not. Therefore, digital signatures can go with an unencrypted or an encrypted message. A user creates a digital signature with a private key that he keeps to himself. He then attaches this signature to a document and sends it to others. His private key is mathematically linked to a public key that he posts on a public key server. He then tells the recipient where his public key is stored. The recipient can then retrieve the sender's public key and reverse the process to determine the authenticity of the document.

A data summary of the information (called a message digest) can be created through the employ of a hash function (called the Secure Hash Standard, or SHS). The data summary is used in conjunction with the digital signature algorithm to create the digital signature that is sent with the message. Signature verification involves the use of the same hash function.

The integrity of a digital signature can be compromised if someone gains illegal access to the computer that runs the encryption software. In common, there are three common reasons for applying a digital signature to communications:

1. Authenticity: Public-key cryptosystems allow encryption of a message with a user's private key.
2. Integrity: Both parties will always wish to be sure that a message had not been altered during transmission. Encryption of the message makes it difficult for a third party to read it, but that third party may still be able to modify it, possibly maliciously.
3. Non-repudiation: In a cryptographic context, the word repudiation refers to the act of disclaiming responsibility for a message (that is, claiming it was sent by a third party). A message's recipient could insist the sender attach a signature in order to prevent later repudiation, since the recipient may show the message to a third party to reinforce a claim as to its origin. Loss of control of a user's private key will mean that all digitally signatures using that key become suspect.

3. METHODS OF PROTECTION

In the previous section a brief description of some threats that any organizations could face when connected to the Internet. In this section a brief description about some methods of protection that could be used to encounter any attack comes from the Internet.

3.1 CRYPTOGRAPHIC TECHNIQUES

Authentication, confidentiality and data integrity can be addressed by studying cryptographic techniques [15]. In using such techniques, it is predictable that information in transmit through the Internet can bypass through various computers before it arrives its target. A malicious user of any of the intermediary computers can monitor the Internet traffic, eavesdrop, intercept, change or replace the data through its entire path. Cryptographic techniques can be used to protect these data. Encryption is the process that makes information indecipherable (cipher text) unless having a decryption key [16]. It uses mathematical algorithms and processes to convert intelligible plain text to unintelligible cipher text and vice versa [17]. It can, therefore, reduce risks from an eavesdropping on a network.

There are two types of key encryption systems: symmetric and asymmetric systems [18]. Asymmetric Key Coding System, which is also commonly called as the Public Key Coding System (PKCS) [19]. The public and private keys are mutual in the RSA algorithm. Thus, if one is used to encrypt, the other can be used to decrypt. In this method it is assumed that the individual is the only one capable of encryption the message with his own private key, but anyone with the mutual public key may decrypt the message. If the message has been published or broadcast, anyone receiving it can be satisfied that the first party performed the encryption and no one else. This is similar to a signature on a document, and has become known as a “Digital Signature (DS)”. Digital signatures can be used to provide authenticity.

Privacy and authenticity can both be accomplish by using the similar pair of keys for each. Still, it may be more appropriate to keep one key pair for privacy and to use another for authenticity. The reason for this apparently inefficient behavior becomes apparent when considering either key enforced decryption of private material.

Conventional encryption is still be used because it is more efficient. The best asymmetric methods are much slower than strong symmetric methods. This is why PGP [20] uses both. When it is used for privacy, the PGP program chooses a 128 bits random number, called a “session key” and uses that as the key for IDEA to encrypt the bulk of the message. It then encrypts the relatively small session key with each of the public key of the intended recipient and adds it to the encrypted data. The recipient, on receipt of the message, can then use their private key to decrypt the session key and use that to decrypt the main information.

3.2 FIREWALLS

Another techniques for protection resources from un authorized user is deploying firewalls. Firewall is a barrier between corporate network and the Internet [21]. It is a set of hardware and software that divide and separate a local area network (LAN) into two or more divisions to bring more security to the resources of the organization [22]. Therefore, the goals of firewall are to restricting people to entering at a carefully controlled point, to protecting network from intruders and to restricting people to leaving at a carefully controlled point [23].

3.3 IDS AND VPN

Another security technique called " Intrusion Detecting System" (IDS) used to detect the harmful and malicious activities, network and system monitoring. This system should have potential to gather and analyze the important transactions and activities such as user access, missing security patches, misconfigured computers, uploading, and downloading [22].

Virtual Private Networks (VPN) uses public networks, tunneling protocols and security procedures to tunnel data from one network to another [22]. The organization can use VPN to protect themselves from the outside intruders [22]. With this tools the communications between the two parties will be mostly secured.

The above discussion related to security organization now could conduct some strategy to protect it self. First organizations need to know all threats and risk that could encounter, and then decide about the protection approach or approaches that described above and select the best tools that could be suitable for them.

Figure 1 below shows the stages that organizations need when they decide to adopt a strategy or tools for the security plans to secure their resources from an outside threats and attacks.

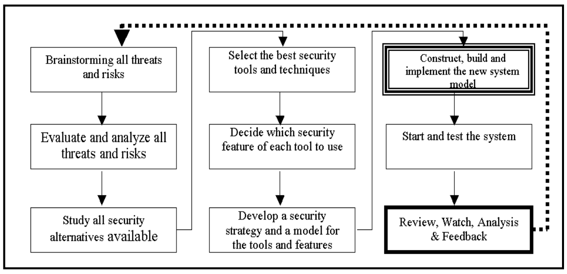
Brainstorming all threats and risks
Evaluate and analyze all threats and risks
Study all security alternatives available
Select the best security tools and techniques
Decide which security feature of each tool to use
Develop a security strategy and a model for the tools and features
Construct, build and implement the new system model
Start and test the system
Review, Watch, Analysis & Feedback

Figure 1: Stages Of Security Building, own model**,**

4. THE PROPOSED MODEL (SMES)

The architecture overview of the proposed model is shown in **figure** 6. This model, the total security model for e-Learning system (**SmEs**) proposes a comprehensive solution for the security problem of the e-education system.

The SmEs model composed of two faces, **figure** 2, the server-side face (SSF) and the client or student-side face (CSF). The architecture of the server-side face is shown in **figure** 4 and the architecture of the client-side face in shown in **figure** 5.

Client-Side Face (CSF)
P2P or Internet Connections
Server-Side Face (SSF)

Figure 2: Interactive Faces of SmEs Model

4.1 THE SERVER-SIDE FACE (SSF)

In the e-education server or SSF a lot of processes and configurations are need to be prepared. These processes and configurations will be briefly discussed in the following sub sections:

• E-LEARNING INFRASTRUCTURE

The SSF is the administration center of the model. It is used for handling student registration, course registration, course payment, as well as course materials hosting and downloading, authentication and authorizations processes. A course launcher (see course launcher section) will be configuring in the SSF to handle courses submitted to students. Three types of databases will be prepared in the SSF: Course Packages and Course Voucher databases, and Students' Database (see course voucher, and course package section). The electronic content of each course (e-course) is saved in the Courses Package Database. The Course Voucher database contains information related to courses, private key, and students' payment fees. A Course Launcher is used to submit e-Courses packages to authorized and registered students. The Students' database will be prepared to contain all potential students' profile, which include information about each student such as: student name, address, ID, Passport ID, etc.

The SSF should be prepared so as to configure all infrastructures needed related to databases for courses packages and voucher and students' profiles.

• COURSE VOUCHER AND COURSE PACKAGE

When the e-course launcher is used to launch the e-course, two objects must have been created for the specified e-course: the course package and the course voucher.

Each course had a course voucher, which contains related information to the specific course such as: course name, course number, voucher number and key information. It contains the encryption key for decrypting the Course Package. This means that, for viewing the e-course material, student must have both the Course Package and the Course Voucher for the specific course. Once the e-Course is successfully launched, the Course Package will be available and could be downloaded by authorized students.

The course launcher will send the course voucher and course package encrypted using the private key of the specific course (Kpr) to the authorized student. The course voucher is supposed to be encrypted using the private key of the course (Kpr) and will be stored in the courses database. The authorized student can download the course voucher, decrypt it using his public key to get the private key, which he can be used to decrypt the course package and eventually view it using his computer, see figure 3. To get this available e-Course, student is supposed to have been registered for it (for more details please see the "Course Registration" section).

With this mechanism, the e-course material will be fully protected. The Course Voucher (cV) and the Course Package (cP) are encrypted using a public key of the student and sent to him. The course voucher encrypted with the student's public key E(cV)Kpu. All these operations of encryption and decryption will be done automatically by the course launcher after the student request the e-course when completing the course registration.

Kpr = E(cV)Kpu ➔ Course Package = D(cP)Kpr

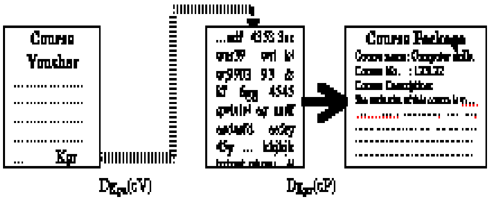

Figure 3: The Mechanism Of Viewing The E-Learning Contents, own model

• STUDENTS' DATABASE

Within this model, the students' database contains the core information about all registered students. It contains information such as: student name, address, passport number, key information and distribution. Additionally, each record about each student contains information about the student's computer hardware configuration, which will be captured during establishing connection between SSF and CSF. All these information will be used for the authentication and authorization process. The SSF will store all the mentioned information in the database in an encryption format.

Certificates and keys belonging to the students are encrypted and stored in the database. Rules set by the SSF regarding authorizations granted or to be granted are stored in the database. Data regarding authorizations such as those revoked or expired dates are stored in this database.

• COURSE LAUNCHER

When an e-Course is created and designed, two objects, the Course Package and the Course Voucher, will be created from the e-Course material. The Course Launcher will send these two objects encrypted using the public key of the student. to the students computer. These two files will be decrypted using the software, which was installed into the students computer (see Course Registering & Paying section), which is a module integrated into the SmEs System (see figure 2). Under the Voucher Administrator, the objects are stored in a database and made available for students to download.

The other part of the SmEs model is the student or client side face, which composed of the following processes, and operations:

• DSS FOR STUDENT

Each student who completes the registration and the fees payment will be granted a public key and a Digital Signature, which he can use to sign and decrypt documents (Course Voucher, Courses Packages, announcements, courses details, grades etc.) send to him by the e-learning system in the server side face.

The RSA cryptosystem is a public-key cryptosystem that will be used to present both encryption and digital signatures (authentication). Digital signatures are generated through SSF, as well as verified. Signatures are generated in conjunction with the use of a private key; verification takes place in reference to a corresponding public key. Each signatory (Registered student) has his own-paired public (known to the public) and private (known only to the student) keys. Because an authorized student using his private key can only generate a signature, the corresponding public key can be used by anyone to verify the signature.

The process for sending a digitally signed encrypted message is similar. In this case, the sender (SSF) must retrieve the student's public key from the student's database. Then uses it to encrypt the document and send it to the student (CSF). The student (CSF) then uses her own private key to decrypt the document, and with this mechanism the e-learning will be sure that only the recipient student can read it, thus, integrity, confidentiality and attenuation will be assured. Additionally, the digital signature provides another advantages, the non-repudiation. In a cryptographic context, the word repudiation refers to the act of disclaiming responsibility for a message (ie, claiming it was sent by a third party). The mechanism strategy in the SmEs model insist that the student attach a signature in order to prevent later repudiation, since the e-learning institute may show the message to a third party to reinforce a claim as to its origin.

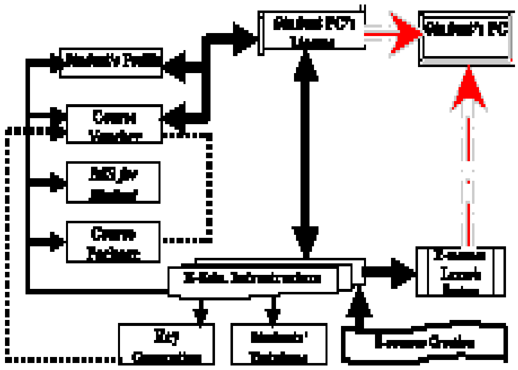

Figure 4: Server-Side Face Architecture(SSF), Own Model

4.2 THE STUDENT- (CLIENT) SIDE FACE (CSF)

The other part of the SmEs model is the student or client side face (CSF), which composed of the following processes, and operations, please see figure 5:

- **Course Registering & Paying**

First of all, student who wishes to enroll in any program using the e-learning system has to contact the institute using e-mail or any other communication channel. During this first contact the student must fill an application form. This application form is used to gather important information about students such as name, e-mail, passport number etc. After that student has to pay for the registration and courses fees using secure electronic payment system. Then, the SSF will send to the registered student (CSS) a software attached with his e-mail. The student to conduct all learning and educational activities will use this software. This software will automatically generate private and public keys for the student. A copy of the public key will be sent to the SSF to be kept in the student' database and course voucher.

To register for an e-Course, the student has to invoke the e-learning platform (SSF) (see Figure 5). The SSF will establish a secure communication connection with the Course Voucher administrator to obtain the Course Voucher. The Voucher administrator will validate the student's Computer License sent by the Course Downloader and encrypt the voucher with the student computer's public key. The encrypted Course Voucher will be sent to student's Course Downloader, and then stored in the Voucher stored of the student's machine in its encrypted form.

In order to get an available e-Course from the SSF, student has to register for it. Student can download the Course Package and obtain the Course Voucher from the SSF in order to view the course material offline. Student can only download the course voucher one time after charged for obtaining the Course Voucher. The Course Downloader of the CSF handles all the whole process of obtaining the Course Package and the Course Voucher. When the Course Voucher is transported from the SSF to the CSF, the Course Voucher will be encrypted using the student's public key, which can only be decrypted only using his private key. When the CSF receives this encrypted Course Voucher, it will be stored securely on the student's computer in this encrypted form, which can only be accessed by the SSF. When the CSF possesses both the Course Package and the Course Voucher, student can make use of his personal computer for viewing the e-Course material offline. However, the student will not be able to make illegal copy of the e-course (see Course Voucher and Course Package section).

- **Student PC's License (**SPCL)

Potential student registers, fills the required information (Student Profile), pays fees and sends this information to SSF system using his e-mail or any other secure communication channel. The SSF system will receive and saved this information in the students' database. A copy of the student' profile will be sent and saved in the student's personal computer.

Student now will be ready to register the course(s) needed according to his specification. He could invoke the SSF system to register the course. The SSF system will immediately perform an authentication and authorization process. During the student registration process student's profile will be checked from the students' database.

When students first time register and paid fees, the CSF software will be send to him using his e-mail. Student now has to install this software into his computer. During the installation, a public key-pair is generated. A hardware profile copy the hardware configuration of the student's computer is also generated. The public key of the key-pair and this hardware profile are both stored inside a file called student PC's License (SPCL). Besides, some personal information about the student is also stored in this SPCL. This makes the APCL unique to each computer. This SPCL is then sent to the e-learning server. The SSF will verify this SPCL, assign to it an expiry date, and sign it digitally, and send the signed SPCL back to the student's computer. This copy of SPCL will be stored during the student invocation of the SSF system. This SPCL will be checked when the student request the e-course material for viewing. All communication between CSF and SSF will be performing using encryption techniques to guarantee secure transferring of information between the two sides.

- **Requesting and Viewing e-Course**

When a student (CSF) invokes the e-learning Platform (SSF) for viewing the e-course material, the student PC's License (SPCL) will first be examined and checked if this invocation is valid. The student will be allowed to access and have a copy of the e-course material if and only if the following conditions are satisfied:

The student PC's license file has not been expired yet.

The student PC's license file had properly signed by the e-learning server.

The software is invoked on the computer on which it was originally installed

During the invocation, a hardware configuration profile of the student's PC (HCPS) will be generated to test the saved copy of the HCPS. This current HCPS is compared with the saved copy of the HCPS that had been stored in the student PC's License (SPCL). The third condition will only be satisfied if the two hardware profiles files are matched.

In addition, the SPCL is designed to have an expiry date. The average lifetime of the SPCL is six months. Before SPCL expires, the SSF will keep track of SPCL, and make sure that there is only one valid SPCL for each student. In a case where a student cheats and request for re-issuing SPCL, or the student's private key is compromised, the old

SPCL will be cancel, however, the student have to pay the registration fees once time again if he want to have another copy of the e-course material.

To guarantee the security of the system, and to ensure the e-Course is well protected, these two processes will go through a special authentication process to mutually authenticate each other. When this authentication process is done, the Voucher Store will use the computer's private key to decrypt the Course Voucher, which was previously encrypted by the SSF using the computer's public. Eventually, the Voucher Store will release the decrypted Course Voucher in the student's computer where it will be used for decrypting the Course Package.

Online Submission Of Assignments

The online learning system involve a variety of communication flows between the SSF and remote students (CSF), each of which may have different security requirements:

general broadcasts (e.g. lectures, module material);

student-specific (e.g. assignment grades);

submission (e.g. work for assessment);

interactive (e.g. tutorials).

To make the communication between CSF and SSF more trustees, each student will be granted a unique public key. Student to digitally sign every document he sends to the SSF must use this public key.

The CSF will help students to solve and submit homework assignments encrypted using their own private key. This will give great opportunity to e-education institute to force their students not to repudiate any document sent by them with their distinctive signature.

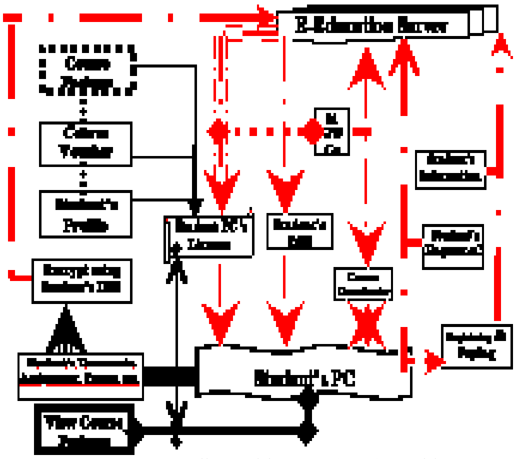

Figure5: Client-Side Face (CSF) Architecture

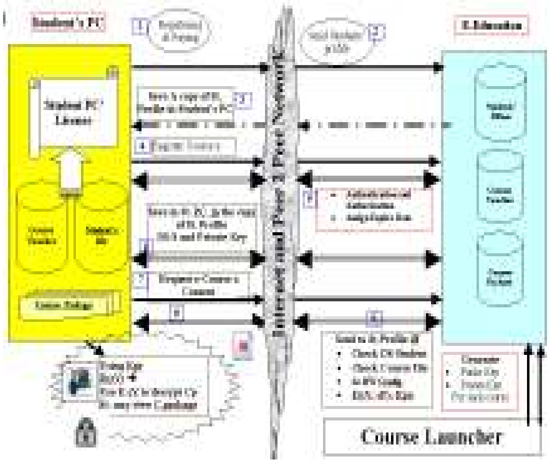

Figure 6: The Architecture Overview Of The Proposed Mode, Own Model

5. CONCLUSION

In this paper, we proposed a new model to make all e-learning process more secure and more trustee. The SmEs model is a comprehensive security framework design to present solution to copyright protection, communication and interaction by both parties the student sand the e-institute.

In order to provide effective support and protection for e-learning facilities, the SmEs model proposed to be used in the e-learning management system. In this model encryption is the solution to protect the contents and all files or messages from reading, copying or stealing.

In the proposed solution, asymmetric encryption-based techniques to satisfy the authentication and non-repudiatory security needs, and use symmetric encryption to meet confidentiality needs.

This research recommends the use of SmEs for the e-learning management system an entity to provide security management features within a system approach. A framework for utilizing such an approach in a distributed computing environment is still being developed in our research.

We finally can conclude that, evolving risks and technology will force e-educational institute to think deeply to use adequate protecting Internet security. Many organizations have produced various methods, strategies, tools, and standards to improve security. Unfortunately they still subsequently can be compromised by brute-force analysis.

REFERENCES

[1] Schocken, S. (2001), "Standardized frameworks for distributed learning", Journal of Asynchronous Learning Networks, Vol. 5 No.2, pp.97-110.

[2] Yau, J.C.K., Hui, L.C.K., Cheung, B.S.N., Yiu, S.M., Cheung, V.L.S. (2002), "A cryptographic schemes in secure e-Course eXchange (eCX) for e-Course workflow", Conference Proceedings of SSGRR 2002 (Summer) International Conference on Advances in

Infrastructure for e-Business, e-Learning, e-Science, and e-Medicine on the Internet (SSRGG 2002s), L'Aquila, Italy, 29 July-4 August.

[3] Phillips, T. "System Security in the National Information Infrastructure: Networks at Risk", NCSA Conference Proceedings, April 1995.

[4] Efrain Turban, David King, Dennis Viehland, Jae Lee, 2006, "E-Commerce A managerial Perspective", Prentice Hall, U.K, London.

[5] Allen, M. W. Michael Allen's, 2003, " Guide to e-learning ". Hoboken, NJ: John Wiley and Sons, 2003.

[6] David G. Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, Mario Piattini, 2006, ""security patterns and requirements for internet-based applications", Volume 16 Number 5 2006 pp. 519-536 , Emerald Group Publishing Limited ISSN 1066-2243

[7] Ethan Sanderson, Karen A. Forcht , 1996, "Information security in business environments", Volume 4 Number 1 1996 pp. 32-37

[8] Furnell, S. (1999), "Security considerations in online distance learning", Proceedings of Euromedia 99, pp.131-5.

[9] McLeod, R, Schell, G (1997), "Management Information Systems", Prentice-Hall, Englewood Cliffs, NJ

[10] Scambray, J. et al. (2001), "Hacking Exposed: Network Security Secrets & Solutions", 2 ed, United State of America: McGraw-Hill, Inc.

[11] Baker, D., Manning, S., Meyer, K., Schaeffer, S., (1995), "Addressing threats in World Wide Web technology", 11th Annual Computer Security Applications Conference, pp.123-3.

[12] Zwicky, E.D. et al. (2000), "Building Internet Firewalls", 2ed , Sebastopol: O'Reilly & Associates, Inc.

[13] R.L. Rivest, A. Shamir, and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM (2) 21 (1978), 120-126.

[14] Stallings, W. 1999, "Cryptography and Network Security: Principles and Practice", 2nd ed., Prentice-Hall, Engelwood Cliffs, NJ, .

[15] Needham, R.M., Schroeder, M.D. (1978), "Using encryption for authentication in large networks of computers", CACM, Vol. 21 No.12, .

[16] Chou, D. C. et al. (1999), "Cyberspace security management", Industrial Management & Data Systems, Volume 99, Number 8, pp. 353-361, available at: **http://ejournals.ebsco.com/direct.asp**?ArticleID=E35WHE69Q8AW23NFTVNX

[17] RSA Security (2003), "Understanding Public Key Infrastructure (PKI)", RSA Security Inc., available at: **http://www.computel.com.lb/Downlo**ads/PKI.pdf

[18] Schneier, B. (1996), "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd ed., John Wiley , Sons, New York, NY, .

[19] Adams, C., Farrel, S. (1999), "Internet X.509 Public key infrastructure certificate management protocols", RFC1421 of IETF, available at: www.ietf.org/rfc/rfc2510.txt/, .

[20] www.pgp.com

[21] Wen, H.J. and Tarn, J.M. (1998), "Internet security: a case study of firewall selection", Information Management & Computer Security, Volume 6, Number 4, pp. 178-184,

[22] Hawkins, S., Yen, D.C. and Chou, D.C. (2000), "Awareness and challenges of Internet security", Information Management & Computer Security, Volume 8, Number 3, pp. 131-143.

[23] Zwicky, E.D. et al. (2000), "Building Internet Firewalls",2 Ed, Sebastopol: O'Reilly & Associates, Inc.