MỘT SỐ VẤN ĐỀ BẢO MẬT TRONG HỆ THỐNG ĐÀO TẠO E-LEARNING

Hồ Văn Ngọc
Trường Đại học Văn Hiến
NgocHV@vhu.edu.vn
Ngày nhận bài: 14/11/2016; Ngày duyệt đăng: 24/11/2016

TÓM TẮT

E-Learning là một hệ thống học tập trực tuyến đang ngày càng phát triển và được coi trọng trên thế giới cũng như ở nước ta hiện nay. Đây là hình thức học tập mới và hiệu quả dựa trên nền tảng internet nhằm tiết kiệm thời gian và chi phí cho người học. Để đảm bảo thành công cho hệ thống E-Learning, một trong những yếu tố quyết định là đảm bảo an toàn và bảo mật cho hệ thống. E-Learning cần phải có một môi trường được bảo mật tốt để cho nó hoạt động và phát huy tất cả chức năng của nó. Trong bài báo này, người viết đề cập đến một số vấn đề an toàn và bảo mật trong hệ thống đào tạo trực tuyến E-Learning.

Từ khóa: *E-learning, an toàn, bảo mật, học tập trực tuyến.*

ABSTRACT

Security issues in E-Learning system

E-Learning is an online learning system which has been growing and appreciated in the world as well as in our country today. This is a new and effective form of learning based on internet basis in order to save time and costs for learners. To ensure the success of E-Learning system, one of the decisive factors is to guarantee the safety and security of the system. It is necessary for E-Learning to have a good secure environment in working and developing all its functions. In this article, some safety and security issues in E-Learning online training systems are mentioned.

Keywords: *E-Learning, safety, security, online training.*

1. Giới thiệu

Đào tạo trực tuyến là sản phẩm của ngành công nghệ thông tin. Từ khi internet ra đời, hình thức đào tạo này được phát triển và cải tiến rất nhiều nhằm đáp ứng nhu cầu học đa dạng của con người. Nền tảng của nó dựa trên web và các kỹ thuật internet để cải tiến và nâng cao việc dạy và học. Công cụ học tập chủ yếu là máy tính. Môi trường học là mạng máy tính và internet. Hiện nay, máy tính và smartphone đang trở nên phổ biến, điều này giúp người học có thể dễ dàng học tập mọi lúc, mọi nơi, nhất là đối với các đối tượng không có thời gian trực tiếp đến trường.

Nhiều tổ chức và trường học hiện đang áp dụng và khai thác rất tốt loại hình học tập trực tuyến E-Learning này. Tuy nhiên, hầu hết các hệ thống đào tạo trực tuyến hiện nay chưa chú trọng nhiều đến vấn đề an toàn và bảo mật, điều này tiềm ẩn các mối nguy cơ rất lớn, có khả năng ảnh hưởng đến sự thành công của hệ thống đào tạo này. Có nhiều yếu tố góp phần tạo nên sự thành công của hệ thống E-Learning, một trong những yếu tố quan trọng nhất là sự an toàn và bảo mật của hệ thống.

Xét về bản chất, E-Learning là hình thức học tập qua mạng internet dưới dạng các khóa học và được quản lý bởi một hệ thống quản lý học tập, đảm bảo sự tương tác và hợp tác giữa người dạy và người học, đáp ứng nhu cầu học mọi lúc, mọi nơi của người học.

Các thành phần chính trong một hệ thống E-Learning bao gồm:

- Internet
- Các khóa học
- Hệ thống quản lý học tập
- Sự tương tác, hợp tác trong học tập

Mặc dù internet là nơi có thể tìm kiếm nhiều thông tin và tri thức cần thiết, nó cũng là nơi tập trung rất nhiều hoạt động bất hợp pháp và tiềm ẩn rất nhiều nguy cơ đối với thông tin được lưu trữ trong máy tính. Bởi vì đào tạo trực tuyến phụ thuộc vào internet và các ứng dụng trên web cho nên vấn đề an toàn trong môi trường đào tạo trực tuyến cũng bị ảnh hưởng, ví dụ như: các tấn công liên quan đến phần mềm và dữ liệu (worms, viruses, macros, denial of service), gián điệp, các hành vi trộm cắp, các lỗi phần cứng,... Tuy rằng rất nhiều người có thể thấy được các mối đe dọa

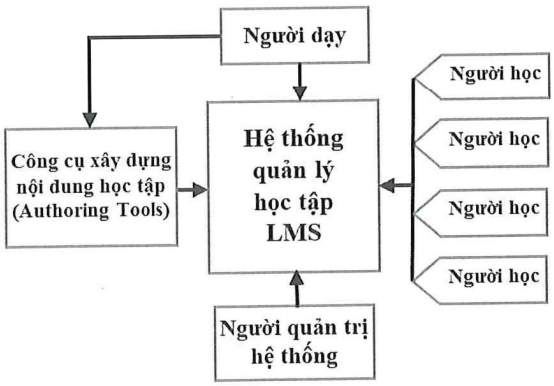
này, hiểu được hậu quả của chúng nhưng lại có rất ít nỗ lực và hành động để khắc phục vấn đề này.

An toàn trong môi trường đào tạo trực tuyến cần phải được quan tâm và đề cao để tránh các mối đe dọa và đảm bảo an toàn cho môi trường học, góp phần phát triển và ổn định lâu dài cho phương pháp đào tạo này.

2. Mô hình hệ thống đào tạo trực tuyến E-Learning

Có nhiều mô hình và ý tưởng về hệ thống E-Learning, mỗi mô hình có ưu điểm, khuyết điểm khác nhau. Phụ thuộc vào điều kiện và đặc thù của mỗi đơn vị chủ quản (tổ chức, trường học) mà sự chọn lựa hệ thống E-Learning có khác nhau. Hình 1 mô phỏng một hệ thống E-Learning khá phổ biến đang được nhiều tổ chức và trường học áp dụng.

Trung tâm của hệ thống đào tạo trực tuyến E-Learning là hệ thống quản lý học tập LMS (Learning Management System). Dựa vào đó, người dạy, người học và người quản trị hệ thống đều có thể truy cập vào hệ thống này với những mục tiêu khác nhau. Một bộ công cụ xây dựng nội dung học tập được áp dụng để giúp người dạy xây dựng nội dung bài giảng phù hợp với tiêu chí giảng dạy E-Learning, bao gồm slide bài giảng, hình ảnh, âm thanh, video, hiệu ứng,... Tất cả các thành phần trên đều nhằm mục đích đảm bảo hệ thống hoạt động ổn định và việc dạy học diễn ra hiệu quả, chất lượng, đáp ứng tốt nhu cầu của người học.



Hình 1: Mô hình hệ thống E-Learning

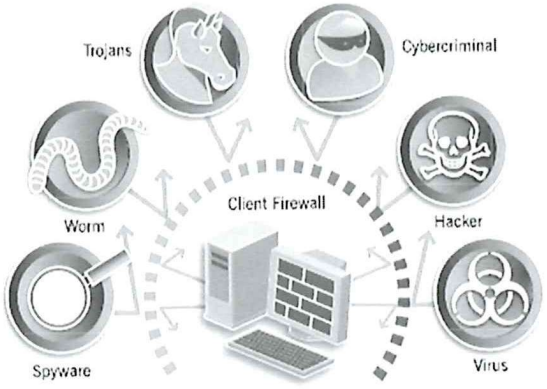
3. An toàn và bảo mật hệ thống E-Learning

3.1. Các mối đe dọa hệ thống E-Learning

Các mối đe dọa đến hệ thống E-Learning đang không ngừng phát sinh theo nhiều cách khác nhau và ngày càng tinh vi, chúng nhằm mục đích làm trở ngại việc dạy và học, đánh cắp thông tin, phá hủy thông tin và gây hại hệ thống. Những mối đe dọa này có thể gián tiếp hay trực tiếp. Khi triển khai hệ thống đào tạo E-Learning, chúng ta cho phép người học sử dụng máy tính, smartphone kết nối vào hệ thống. Điều này dẫn đến rất nhiều mối đe dọa có thể phát sinh.

Các đe dọa từ phía người học

Máy tính của người học có khả năng không đảm bảo an toàn. Hình 2 nêu ra một số mối đe dọa thường gặp đối với máy tính.



Hình 2: Mô phỏng các mối đe dọa thường gặp đối với máy tính

Thay đổi trái phép

Hiện nay, có một số trang web xuất hiện thông tin không chính xác, đó là hệ quả của việc nội dung bị thay đổi trái phép bởi hacker hay các user khác (trái phép). Điều này làm cho người sử dụng không tin tưởng vào tính chính xác và nhất quán của dữ liệu. Vấn đề này càng đặc biệt nghiêm trọng đối với hệ thống E-Learning, bởi vì nội dung đào tạo, kiến thức được đưa ra từ hệ thống đến người học phải chính xác; nếu không, hệ thống E-Learning sẽ bị phá sản (Naserasadi, 2011).

Sử dụng trái phép

Tài liệu số và nội dung bài giảng được lưu trữ trên hệ thống E-Learning. Người học có thể tìm cách sao chép trái phép các nội dung này và phân phối đến nhiều người dùng trái phép khác.

Xâm nhập trái phép vào hệ thống

Hệ thống E-Learning bao gồm nhiều máy tính, những máy tính này có thể có những điểm yếu mà hacker có thể lợi dụng để tấn công và xâm nhập, nhất là các máy tính của nhân viên trong hệ thống, ví dụ như: một số port trong máy tính ở trạng thái mở mà người sử dụng không

biết, máy tính có thể bị nhiễm virus, spyware trong quá trình sử dụng, máy tính đang sử dụng một số phần mềm không rõ nguồn gốc có tiềm ẩn các lỗ hổng,... Thông qua các điểm yếu này, hacker có thể tìm cách xâm nhập và gây hại cho hệ thống.

Ngăn cản tiến trình học tập

Đây là hành động phá hoại, gây cản trở việc triển khai nội dung học đến người học theo đúng khung giờ và điều kiện đã định trước. Như thế, phần nội dung bài giảng này sẽ mất giá trị, ảnh hưởng đến lịch học, khiến người học không hài lòng. Một ví dụ cho trường hợp này là tấn công DoS - Denial of Service (Naserasadi, 2011).

3.2. Phân tích rủi ro

Phân tích rủi ro là một xử lý quan trọng trong mọi dự án (Naserasadi, 2011). Cần phải tiến hành phân tích rủi ro để dự kiến được những rủi ro nào có thể xảy ra, qua đó đánh giá mức độ ảnh hưởng của rủi ro nếu nó xảy ra. Rủi ro luôn tồn tại trong mọi dự án, ta không thể phát hiện tất cả rủi ro, cũng không thể loại bỏ tất cả rủi ro, chỉ có thể tìm ra các giải pháp để giảm thiểu rủi ro. Trong số những rủi ro mà ta dự kiến được, cần phải phân loại chúng để đưa ra độ ưu tiên cho từng loại rủi ro, từ đó tính ra thiệt hại dự kiến của nó theo công thức:

$$e = v * p$$

Trong đó: e là thiệt hại dự kiến của rủi ro, v là giá trị tài sản và p là xác suất có thể xảy ra rủi ro (Greene và Stellman, 2006; Schneier, 2003).

Rủi ro đến từ nhiều thành phần, liên quan đến nhiều đối tượng tham gia trong hệ thống. Sau đây là một số rủi ro cần quan tâm:

Tài liệu, nội dung học tập

Tài liệu học có thể đến tay của người học không hợp lệ và có thể bị sử dụng sai mục đích. Do đó, hệ thống cần phải đảm bảo chỉ có người học hợp lệ mới nhận được nội dung học và nội dung này không thể bị thay đổi, đồng thời hệ thống cũng có cơ chế giúp người học kiểm tra được tính toàn vẹn của nội dung học.

Công nghệ, qui trình dạy học

Một số tổ chức có thể tự xây dựng hoặc mua nội dung, bài giảng của các khóa học và công nghệ dạy học từ các tổ chức khác, do vậy chúng cần phải được bảo mật. Để đáp ứng yêu cầu này, một số qui định cần phải được áp dụng cho tất cả thành viên của hệ thống, trong đó người dạy là đối tượng cần phải tuân thủ đúng các qui định về bảo mật. Để thực hiện tốt việc này, cần thành lập một đội ngũ để phụ trách và quản lý.

Môi trường và điều kiện dạy học

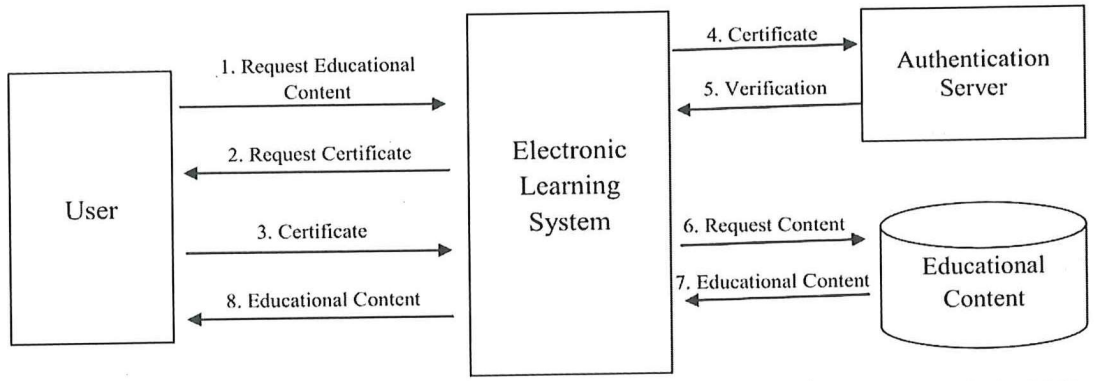
Người học có thể ở bất cứ nơi đâu và bất kỳ lúc nào cũng có thể tham gia vào hệ thống học tập, chỉ cần họ có kết nối internet và thiết bị học (máy tính, smartphone,...). Để thuận tiện cho người học, hệ thống cần phải đảm bảo hoạt động liên tục, kể cả các kết nối internet cũng phải luôn được duy trì. Tuy nhiên, việc kết nối internet bị gián đoạn hay mất nguồn điện là điều có thể xảy ra bất cứ lúc nào, điều này ảnh hưởng rất nhiều đến người học. Để hạn chế các rủi ro này, tổ chức cần phải có đường truyền internet dự phòng, nên có nhiều đường truyền internet từ nhiều nhà cung cấp khác nhau. Tổ chức cần trang bị hệ thống lưu trữ điện UPS phục vụ cho các máy chủ và máy phát điện dự phòng để cung cấp điện ổn định cho cả hệ thống E-Learning. Bên cạnh đó, để dự phòng các sự cố của hệ thống có thể xảy ra, tổ chức cần phải chú trọng đến việc thường xuyên và định kỳ backup dữ liệu và hệ thống.

3.3. Biện pháp bảo mật hệ thống E-Learning

Việc xây dựng nội dung đào tạo trong hệ thống E-Learning thực sự rất phức tạp, tiêu tốn rất nhiều thời gian và công sức. Nội dung dạy học có thể bao gồm: văn bản, hình ảnh, âm thanh, phim,... Dựa trên một số nghiên cứu gần đây, 80% cuộc tấn công trong hệ thống E-Learning được thực hiện bởi những người bên trong tổ chức (Graf, 2002; Naserasadi, 2011). Do đó, bên cạnh việc đảm bảo an toàn cho hệ thống từ bên ngoài thì việc sử dụng một số kỹ thuật như: mã hóa dữ liệu, chữ ký số, Virtual Private Networks là cần thiết để bảo vệ dữ liệu bên trong. Sau đây là một số biện pháp bảo mật.

Mã hóa dữ liệu

Trong hệ thống E-Learning có nhiều thông tin quan trọng như: thông tin của người học, tư liệu, bài giảng, qui trình công nghệ,... Những thông tin này cần phải được mã hóa theo một chuẩn thích hợp. Việc mã hóa áp dụng cho dữ liệu lưu trữ trên các thiết bị và cho cả dữ liệu truyền tải trên mạng. Quá trình mã hóa và giải



Nguồn: Naserasadi A., 2011.

Hình 3: Sử dụng chứng thư số để bảo vệ nội dung E-Learning

mã được tiến hành tự động trên máy chủ, người học không nhận biết điều này. Một vấn đề khác cần phải lưu ý đó là máy tính của người học có khả năng cache dữ liệu và lưu giữ chúng tạm thời. Để giảm khả năng dữ liệu bị lấy cắp, nên thiết lập thời gian sống của dữ liệu (data expire) phù hợp và giới hạn việc cache dữ liệu.

Bảo vệ văn bản

Văn bản là dạng dữ liệu thông dụng nhất và dễ sử dụng nhất trong hệ thống E-Learning, nhưng nó cũng dễ bị đánh cắp và phân tán nhiều nhất. Để bảo vệ văn bản tránh khỏi các xâm nhập từ bên ngoài hệ thống và sử dụng trái phép, ta có thể sử dụng kỹ thuật AAA (Authentication, Authorization và Access control) (tương ứng là: Xác thực, Kiểm soát và Điều khiển truy cập). Cụ thể, ta có thể sử dụng một số cơ chế như: username và password, thẻ nhận dạng thông minh (Smart Identification Card) hay phương pháp nhận dạng sinh trắc học (Biometric Identification Methods) (Naserasadi, 2011; Jampour và cộng sự, 2011).

Bảng 1: So sánh các loại nhận dạng khác nhau và các phương pháp xác thực

Method	Information Sources	Accuracy	Reliability	Maintainability	Availability	Upgradeability	Integrity	Cost
Username & Password	9	9	7	10	10	9	7	10
Smart Card	5	10	10	6	5	5	10	6
Hand-Held Password Generator	4	10	10	3	3	4	10	2
Biometrics	5	7	8	5	5	3	8	3
Cryptography	8	9	9	9	8	8	8	10
Place-Based	7	2	2	6	9	9	3	9

Nguồn: Naserasadi A., 2011.

Một cách khác giúp bảo vệ văn bản tránh bị thay đổi trái phép là chuyển văn bản sang định dạng PDF hay sử dụng kỹ thuật chứng thư số (digital certificates) để bảo vệ nội dung dạy học như Hình 3. Mỗi phương pháp bảo vệ này đều có những ưu điểm, khuyết điểm khác nhau, tùy vào từng trường hợp và điều kiện cụ thể. Bảng 1 so sánh một số phương pháp bảo vệ dựa trên 8 tiêu chí: nguồn thông tin (information source), tính chính xác (accuracy), độ tin cậy (reliability), khả năng bảo trì (maintainability), khả năng sẵn sàng (availability), khả năng nâng cấp (upgradeability), toàn vẹn hệ thống (system integrity) và chi phí (cost) (Guttman và Roback, 2001; Naserasadi, 2011).

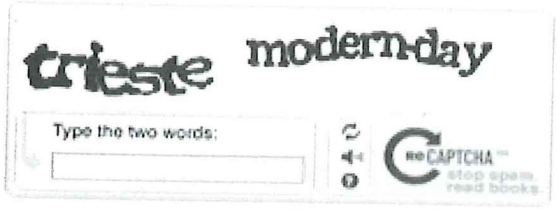
Xác nhận người học bằng phương pháp login

Việc kiểm tra và xác nhận người học có hợp lệ hay không là rất cần thiết, nhằm loại bỏ những người học trái phép (không đăng ký, hacker), đảm bảo nội dung học được phân phối đúng người. Để đăng nhập vào hệ thống E-Learning, người học sử dụng giao diện web. Thông thường người học chỉ cần cung cấp 2 thông tin là username và password.

Tuy nhiên, hiện nay có một số công cụ phần mềm, do một số người có ý đồ xấu tạo ra, có khả năng đăng nhập tự động bằng cách thử rất nhiều username và password với mục đích dò tìm ra thông tin đăng nhập vào hệ thống. Để ngăn chặn cách thức đăng nhập bằng công cụ phần mềm này, một giải pháp là sử dụng CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Như vậy, khi người học login vào hệ thống, họ cần phải cung

cấp username, password và xác nhận captcha.

Đặc điểm của captcha: trên vùng captcha xuất hiện một hoặc hai từ khó nhận diện. Các công cụ phần mềm khó nhận biết được nội dung yêu cầu trong khi con người có thể nhận biết được.



Hình 4: Hình ảnh CAPTCHA khi đăng nhập

Trong Hình 4 có hai từ khó đọc là "trieste modern-day".

Theo dõi hình ảnh người học

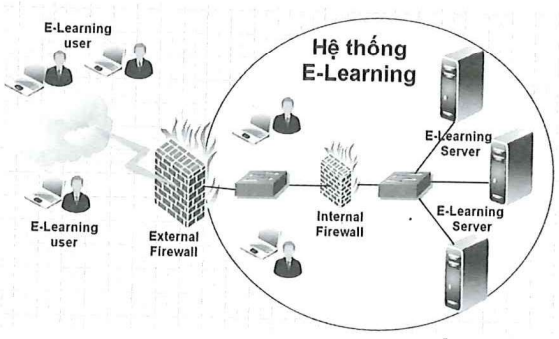
Một phương pháp khác có thể xác nhận người học hợp lệ là ghi hình và hiển thị hình ảnh người học lên hệ thống, chỉ cần hiển thị khuôn mặt. Để làm được điều này, về phía người học phải sử dụng camera ghi hình, có thể sử dụng webcam đối với máy tính hay camera đối với smartphone. Về phía tổ chức, cần phải trang bị hệ thống đủ để hiển thị hình ảnh của tất cả người học. Điều này có ảnh hưởng đến chi phí. Tuy nhiên, có thể mỗi lần chỉ hiển thị hình ảnh của một nhóm nhỏ người học, sau đó định kỳ chuyển sang hiển thị hình ảnh của một nhóm nhỏ khác, cho đến khi hiển thị tất cả hình ảnh của người học.

Biện pháp bảo vệ ứng dụng

Mục tiêu của biện pháp này là ngăn chặn việc sao chép ứng dụng. Hiện nay, việc ngăn chặn sao chép ứng dụng vào các thiết bị lưu trữ như: USB, CD/DVD, Mobile HDD là không thể. Do đó, biện pháp còn lại là khóa các cổng kết nối đến các thiết bị lưu trữ tại các máy tính lưu trữ dữ liệu phục vụ đào tạo và trên máy tính của nhân viên trong hệ thống E-Learning; ví dụ: khóa các cổng USB, chỉ trang bị ổ đĩa CD/DVD readonly. Ngoài ra còn có biện pháp bảo vệ ứng dụng bằng cách sử dụng serial numbers (nhưng cách này cũng có thể bị hacker bẻ khóa sau một thời gian sử dụng). Biện pháp bảo vệ ứng dụng bằng phần cứng cũng rất hiệu quả nhưng chi phí quá cao nên khó triển khai.

Bảo vệ hệ thống mạng

Hệ thống E-Learning gắn liền với hệ thống mạng và internet. Đối tượng phục vụ của hệ thống có thể ở bất kỳ nơi nào trên thế giới chỉ cần họ có thể sử dụng máy tính hay smartphone kết nối đến hệ thống. Do đó, chúng ta khó kiểm soát được tất cả người học, trong số người này có thể có hacker hoặc người có ý đồ xấu muốn gây hại cho hệ thống. Vì vậy chúng ta cần phải tăng cường bảo vệ và kiểm soát các truy cập vào ra hệ thống E-Learning của chúng ta. Một biện pháp hữu hiệu là thiết lập hệ thống tường lửa để kiểm soát truy cập và ngăn chặn các truy cập trái phép.



Hình 5: Mô hình bảo vệ hệ thống mạng bằng tường lửa

4. Kết luận

Xu hướng đào tạo trực tuyến E-Learning đang được nhiều tổ chức, trường học quan tâm. Bộ Giáo dục và Đào tạo cũng đã có chủ trương cho các trường đại học phát triển hình thức đào tạo này. Việc triển khai hệ thống đào tạo E-Learning không quá khó nhưng vấn đề an toàn và bảo mật hệ thống lại rất phức tạp và khó khăn. Cho dù hiện nay đã có không ít cơ quan, trường học triển khai đào tạo E-Learning nhưng họ đều gặp phải khó khăn về an toàn và bảo mật.

Bài báo này đưa ra được một số khó khăn và các mối đe dọa đến hệ thống E-Learning, đồng thời bài báo đã đưa ra được một số biện pháp khả thi nhằm tăng cường mức độ an toàn và bảo mật cho hệ thống. Các vấn đề và các biện pháp an toàn đã nêu trong bài báo có thể áp dụng cho hệ thống E-Learning đang được xây dựng tại Trường Đại học Văn Hiến.

TÀI LIỆU THAM KHẢO

[1] Naserasadi A., 2011. Author's Security in Electronic Learning Systems, *International Journal of Computer Applications*, Vol 2, No 10.

[2] Graf F., 2002. Providing security for e-learning, *Computers and Graphics,* Volume 26, Issue 2, pp.355-365.

[3] Jampour M., Naserasadi A., Estilayee M. and Ashourzadeh M., 2011. Extract and Classification of Iris Images by Fractal Dimension and Efficient Color of Iris, *International Journal of Computer Applications* (IJCA) 18(1), March 2011, pp.11-14, ISSN: 0975-8887, Published by foundation of computer science.

[4] Greene J. and Stellman A., 2006. *Applied software project management,* O'Reilly Media Inc., pp.81-95.

[5] Schneier B., 2003. *Beyond fear: Thinking sensibly about security in an uncertain world,* New York: Springer-Verlag, pp.59-73.

[6] Guttman B. and Roback E. A., 2001. *An Introduction to Computer Security: The NIST Handbook,* National Institute of Standard and Technology, 278p.