Study on Attacks & Protect of e-Learning contents

Nikhilesh Barik
Research Scholar, Burdwan University,
Burdwan, India.
e-mail: nikhileshbarik@gmail.com

***Abstract*—During the last 10 years, significant volume of real life education applications are implemented by the effective use of Information & Communication Technologies (ICT). The number of learners in e-Learning system is also increasing in comparison to the traditional education system. In e-Learning system different documents (e learning contents) like class lectures(audio/video),user personal documents (query /sample answer/rules and regulations etc), texts(class notes, tutorials, questions, etc), images (diagrams /certificates /grade sheets, etc) etc may be required to send among different users like managers to learners, teachers to learners, etc. Storing and protecting these documents from different attacks has become a great challenge. Security became an important issue to protect e-Learning documents, also they can be retrieved, edited and append easily only by the authorized users. In this paper, we are sharing different ways of attacks and techniques to protect e-Learning contents with different access control strategies which basically is a part of implementation of database security, as well as e-Learning security.**

Keywords- e-Learning;e-Learningsecurity;Database-security, e-Learning content.

I. INTRODUCTION

The application of Information and Communication Technology (ICT) in e-Learning environment has brought dramatic changes in higher education. Educational sectors (like universities, colleges, institutions, etc), corporate organizations and other sectors are also changing their policies & updating them according to the current demand of education system like e-Learning, m-Learning, n-Learning etc. All these learning methodologies may be represented by distance learning, online learning, networked learning but the basic objective of all these learning systems is to promote educational interactions between learners, instructors and all other learning communities[1]. Anybody can be enrolled for any kind of degree or simply for enhancing their knowledge irrespective of the place where he/she belongs to.We will use the term learners as students, e-contents as "all documents used in e-Learning system" and users as all kind of learners , teachers, system managers and admin managers .

So we can simply define e-Learning as the electronical learning methodology through internet. As the number of internet users are increasing day by day, e-Learning trend is also increasing rapidly. The diagrams in Figure 1 shows the number of internet users of 5 top countries[14] and Figure 2 shows the increasing inclination of internet users per 100 inhabitants in 2001-2013, in different categories. [100 inhabitants are obtained by dividing the number of Internet subscribers by the population and multiplying that by 100[18].

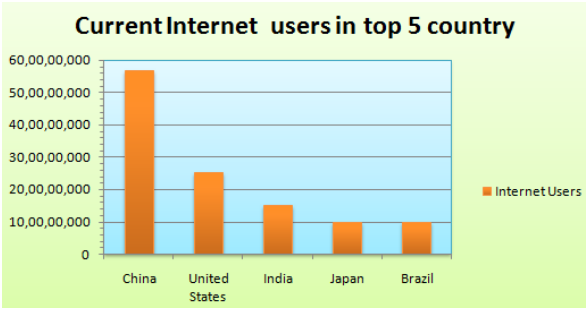
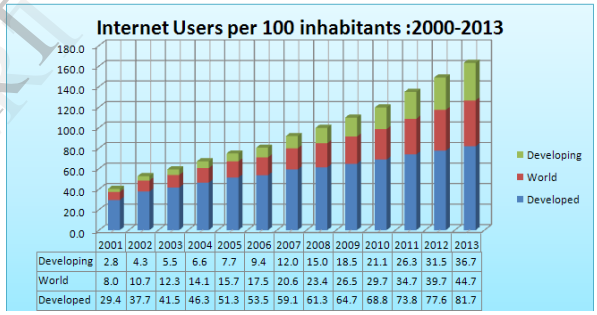


Fig. 1. Five top most countries' internet users



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Developing	2.8	4.3	5.5	6.6	7.7	9.4	12.0	15.0	18.5	21.1	26.3	31.5	36.7
World	8.0	10.7	12.3	14.1	15.7	17.5	20.6	23.4	26.5	29.7	34.7	39.7	44.7
Developed	29.4	37.7	41.5	46.3	51.3	53.5	59.1	61.3	64.7	68.8	73.8	77.6	81.7

Fig. 2. No. of internet users under 3 categories in world (2000-2013)

The concept of higher education system has already changed by the effect of e-Learning, specially with respect to the quality education and support processes with the help of modern technologies. On the other hand, attackers are also developing themselves to crack and break any system by using the same technologies. In e-Learning, attackers can change or modify the authenticated e-contents like learning materials, certificates, question papers, lecture video, mark sheets etc. That is why it becomes an important issue for the researchers to generate new ideas for the protection the e-contents from the attackers. As all the e-contents have been stored in databases, we can say database security will be a prime matter in all concern in the field of computer science.

Many researchers describe database security with different architectures. One of the Simple Database Security Architecture is shown in the Figure 3 [12]. Commonly database security is the application of different cryptographic algorithms e.g. digital signature, digital certificates on databases through network. In this paper, our emphasis is laid on different strategies to store and protect

e-contents to make the system reliable, speedy and efficient against the different attacks. We have also considered four basic security requirements (PINA); Privacy, Integrity, Non-Repudiation and Availability with today's additional demands like data quality, timeliness, provenance and the most important aspects of the data to be complete, correct and up-to-date[2],[13]. Figure 3 represents different e-Learning Database components.

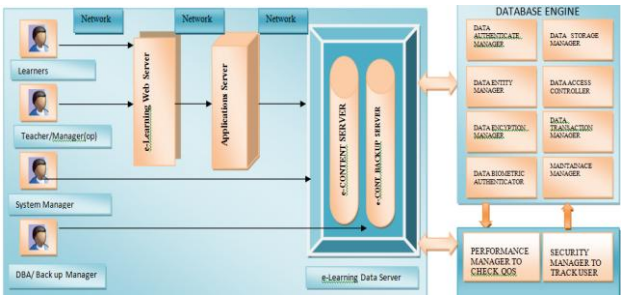


Fig. 3. Architecture of Secure Database in e-Learning application

The second section explains different attacks on databases. Different techniques for implementing security is discussed in section three. Section four elaborates management policies which includes different access control strategies. The fifth section offers a short description of e-content storing. Last section ends with brief conclusion.

II. Different Attacks On Databases

Attackers are more efficient to crack any system with the help of recent technology in comparison to the developers, who create the system. So we must update ourselves regarding the probable attacks on the web servers, application servers and main backup database server. Backup servers are basically used to store e-content system for years after years. Different types of database attacks are described in this section

A. Denial of Service(DOS) and Distributed Denial of Service (DDOS)

Denial of Service (DOS) and DDOS (Distributed Denial Of Service) are common attacks in web applications. After receiving the common e-contents like class notes, certificates etc., it may be declined by the learners. This situation is called Denial of Service (DOS). DOS conditions may be created via many techniques and these are related vulnerabilities. As discussed by Amichai Shulman [15] DDOS may be achieved by taking advantage of a database platform vulnerability to crash a server, data corruption, network flooding in all three application servers, web server and database servers. Protection from these kind of attacks is only possible if there is a checking in each level of accessing and by data integrity rule.

B. Direct Attacks

Direct attacks are obvious attacks and are successful only if the database does not implement any protection mechanism. Generally it does not happen in e-Learning systems as there is login system from each learner and many application program must be written for the verification before accessing the main database server. In direct attack, the attacker once fails to break the desired result from one database, moves to the next database and so on[3].

C. Indirect attacks

Most of the time mark sheets or certificates are not displayed in the website. So attackers are not able to see these contents. Attack on the contents, which are not visible is called indirect attacks[3]. Attackers prefer these type of attacks in most of the cases of e-Learning system. Combinations of queries are used to break the security mechanisms.

D. The fraud learners attack (man–in-the-middle)

Learner attempting to connect to the e-Learning server is forcefully diverted to their own website similar to the organization and as soon as learner enters his details man in the middle (attacker) will try to initiate in the main server.
As a solution, Security Assertion Mark-up Language(SAML) is the standard for exchanging authentication information[8]. Also randomly challenge response system can stop these attacks. Biometric authentication such as fingerprints or iris scanner can be used to see whether the learner is physically present or not.

E. Intellectual attack (SQL Injection)

It is a technique by which attacker modifies the expected input string by the SQL statement. These can be done in many ways like calling stored procedure, at the time of SELECT/INSERT command ,bypassing authentication mechanism. The only way to prevent this SQL injection is to know better about the code for web applications[11],[8].
select * from tablename where some fieldname = '<some SQL statement>;
e.g. select * from login where user like ' " +username+" ';
This SQL code is designed to pull up the records of the specified user from its table of login. The attacker may continue to use code within query strings to accumulate more information from the e-Learning server, they will be treated as authorized learners. For solution biometric authentication can help a bit[16].

III. Techniques To Implement Security

There are many procedures to implement database security to the e-Learning system and its content. Oreally has already discussed some ways to develop security policies of e-Learning system[12]. According to the architecture of secure database in e-Learning system in figure -3, six steps of security techniques are discussed below.

A. Authenticated learners

All the registered learners must be authenticated before granting any kind of roles and privileges to access the server by Secure Sockets Layer (SSL), the host operating system and different network services. Few data like MAC address, current IP, etc. must be stored by the server for each learner,

teacher, and manager also, so that as and when it will be changed, some log files will indicate as security tools.

B. *Authenticated security administrator*

As the database will be large enough, so there must be several types of managers. Among them, the security manager may decide about related privileges to several learners, teachers or other managers. Also security administrator must have some routine jobs like checking log files, ensuring the learner's password's minimum requirements [11] like

i. It should be at least a certain number of characters long
ii. Totally differs from the username
iii. Must have at least one numeric, one alphanumeric, one special character and one symbol created by the administrator related to the course id and date.
iv. Need to change the password after certain number of log in and
v. New password must differ from the previous password by few characters
vi. Best solution is to use virtual keyboard at the time of login with such images which do not exist in standard keyboard.

C. *E-content with Digital Signature or Digital Certificate*

To authenticate a learner and maintain integrity, we need to use digital signature. At the time of delivery of e-certificate, we should use digital certificate using different cryptographic algorithms likes SHA1-RSA, MD5-DSA etc. The following figure-4 shows the sample signed marksheet with SHA1–RSA signature algorithm[4],[6].

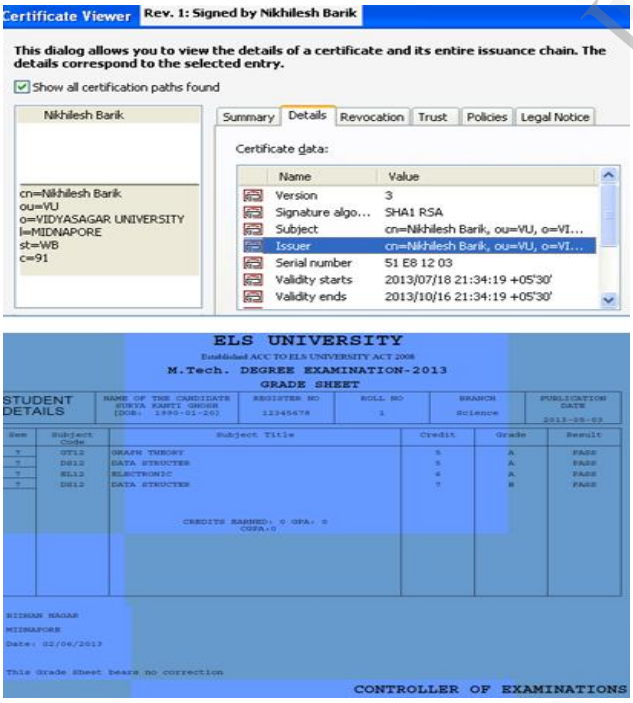


Fig. 4. Signed Mark Sheet to learner by SHA1-RSA Signature Algo

D. *Encryption and e–Learning Database*

It is always better to store all important e-contents like e-Learning certificates or learners credit card number etc. in the encrypted form. Objective of storing in encrypted from is that no member from the core database team also, will not be able to view, access or edit those important data. In this way whenever some fields of a particular table are stored in encrypted form then each field must have some encrypted key. Similarly, a table of decryption key is also required to retrieve those data. There can be a master key for both the purposes but that key has a number of disadvantages also.

E. *Biometric Authentication*

Biometric technology is the other approach of authentication. It is the unique characteristics inherent in human being. This unique physical part provides an assurance about the true identity of an individual. A biometric methodology is a unique pattern-recognition system. Following biometric methods can be used for authentication purposes during any kind of e-content transaction among different entities of e-Learning system[17].

- Fingerprint &Hand geometry

  There are different ways of identifying users according to their fingerprints. One can create a digital image and compare characteristic features. Any of the finger can be used for this purpose. Instead of a single fingerprint, the hand geometry of the entire hand may be used. The advantages are. Less possible error in comparison to particular finger. Hand geometry vary percentage of different people is less in comparison to fingerprint.

- Retina Scan

  Most costly biometric authentication is retina scan. It is safe enough except little bit of fear from the users. It may be used before entering in the examination centre and at the time of collection of final certificate.

- Iris Scan

  A picture of one's eyes can be taken by any high pixel camera and people can be recognized by differences in their iris. In comparison to retina scan, an iris scan is less reliable. The advantage of this method is that the user does not have to look directly into a device and an easy test is possible.

- Facial Recognition

  In the context of e-Learning systems facial reorganization can be used at the time e-assessment. The advantage of this system is the user will not be disturbed at the time of authentication

F. *Office Protocol Maintenance*

In any educational Institute, managers, teachers are using pirated software at their office PC /laptop. They also do not care to log off, when they leave their chair. Even they also share all kinds of passwords when they think it is beneficial for them. Highest level of management needs to be

committed to ensure that the security policy has to be maintained, otherwise some kind of punishment policies must be implemented. Another way of solution is to keep the passwords in the form of biometric mode and automatic log off after a certain duration .There must be implemented some restriction so that no system user can able to access other user's files[5].

IV. MANAGEMENT POLICIES (ACCESS CONTROL)

Access control mechanisms of DBMSs are based on policies which are purely dependent on the concerned organization. Generally database access control depends on the subject's identity and authorization rules. These mechanisms should be flexible so that granting authorizations to the users will be easier. Because of such flexibility, open policies are adopted in many application environments. Any commercial DBMSs also adopt such open policies. Thus flexible access control(FAC) for maintaining authorization policy is becoming an important aspect related to database security[2][10].

A. Flexible Access Control (FAC)

Most of the time mechanisms related to the access control of e-Learning system are flexible so that any of the teachers may be able to allow learners to grant authorizations on the data as and when required. Because of such flexibility, open policies are adopted in many application environments and this is the reason that e-Learning DBMSs adopt such policies like other commercial organisations.

However, the proposed architecture in Figure-3 supports unique authorization methods by accomplishing Level Based Access Control (LBAC).The LBAC uses both Role-based Access Control (RBAC) based on policies and Team-Based Access Control (TMAC).

B. Active Role-Based Access Control (ARBAC)

Depending on the responsibilities of the manager or teachers, this RABC may be implemented. For the examiner point of view, they can edit their question paper up to the last minute. This is mainly used by the majority of e-Learning organizations .Here learners also will be treated as user and every year role of learners will be different, course wise and policy wise. One step Active of RABC can be termed as Active Role-Based Access Control(ARABC). It may be classified in two categories at the time of implementation. Implement mandatory access control(MAC) or discretionary access control (DAC). Basically any access control list(ACL), with respect to a database will be a separate record of that database. The Figure -5 shows the Active Role-Based Access Control with respect to session, course and learner.

C. Team Based Access Control (TMAC)

It is an approach to apply role-based access control in collaborative environments[9]. A team indicates here group of users to look after a specific task. In case of receiving payment from the learners, i.e. finance department, always requires two persons to complete any job. But in case of hybrid task also this concept may implemented.

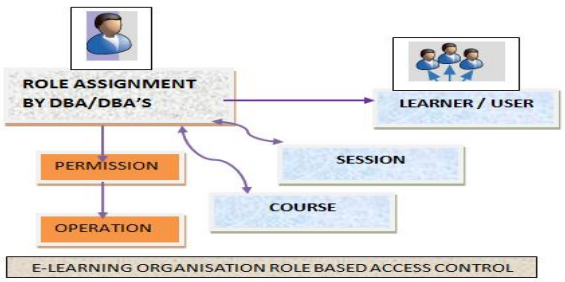


Fig. 5. ARBAC in e-Learning System

D. Level Based Access Control (LBAC)

Depending upon the level of user, this LABC may be implemented. For the end level user i.e. learners may access objects what they had privileges on, or see/read their own data within a given table. For example all level users may be able to edit their password, or contact details, but not their mobile number ,email address or id etc. According to the policies of the e-Learning organization, LBAC may be implemented as two /three checking access controlled, which is popularly known as level Access Based Control Two (LABC-2)/ level Based Access Control Three(LABC-3).

V. E-CONTENT STORING

In e-Learning system most of the e-content will be in the form of multimedia data. There may be few demented (.docx/.pdf) file which may be available in the web server through application server. So the main multimedia database(MMDB) should always be in separate place and not reachable to all users without application program as shown in the Figure2. Storing these kinds of data have lots of problems with transactional update, indexing or retrieving from the learners as well as from teachers. A solution for this problem as suggested by Sudarshan[8] is several issues must be considered when data are to be inserted in a database.

A. Multimedia Data (Audio/Video/Image)

Such very large file (video/ audio/image) could be split into smaller pieces and those smaller pieces can be stored in a database with the concept of indexing. So some index (file name) must be linked with multimedia object. SQL/MED (Management of External Data) allows to retrieve those multimedia object through application program. But in case of audio retrieval minimum bandwidth must be there to avoid gaps in the sound. Also that may require more application program for biometric authentications[8].

E-Learning data must be stored in a compressed format as a very large space is required for it. The Moving Picture Expert Group (MPEG) discovers the way to store continuous video/audio with encoding in MPEG-4 format. To ensure the availability of a standby database, it is required to copy the all regular databases first. This type of database is called remote backup or data guard. This remote back up is very useful when any damage occurs in primary

databases. Basically these servers are used for reporting and support system only.

B. *Lightweight Directory Access Protocol (LDAP)*

Lightweight Directory Access Protocol (LDAP) is another purpose of storing user data in database management system. Directory server and the directory structure are suitable approach for storing user data, which can be retrieved easily through the LDAP protocol by the different e-Learning users[17].

C. *Dedicated server, Data Warehouse and Data Mining*

All the e-Learning organizations must arrange dedicated servers not only for the performance and reliability but for the security reason also. As data warehouse is a collection of integrated databases designed to support managerial decision making and problem solving functions, it will help to store e-content. As nobody else can access this one, no need to share the IP address with other, all kind of special softwares may be used for data mining as and when required. Access control policies will be stronger by using different customized firewalls[7].

VI. CONCLUSIONS

It is clear that the heart of e-Learning security is nothing but database security for an information system. We have discussed in this paper different probable attacks and protection from those attacks, different techniques and functionalities to implement database security. Also discussed multiple access strategies to ensure the secrecy, integrity, and availability of the stored data. Another objective of this paper is that data from the databases should not be disclosed to any unauthorized users by ensuring integrity (cryptographic algorithm required) and providing the storage structure of multimedia database with the availability to the learners who must be able to map their knowledge to the real world.

REFERENCES

[1] Barik Nikhilesh and Karforma Sunil "Risks And Remedies In E-Learning System "International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012 ,ISSN -0974-9330(OL),0975-2307(P), PP 51-59.

[2] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE "Database Security—Concepts,Approaches, and Challenges "IEEE Transactions on Dependable and Secure Computing"; Vol. 2, No. 1, January - March 2005

[3] Emil Burtescu "Database Security - Attacks And Control Methods"Journal of Applied Quantative Methos",Vol4 No 4 ;2008 PP 449-453.

[4] Kahate Atul ,"Cryptography and Network Security" TMH Education Pvt. Ltd , Second edition.2009

[5] P. Missier, G. Lalk, V.S. Verykios, F. Grillo, T. Lorusso, and P. Angeletti, "Improving Data Quality in Practice: A Case Study in the Italian Public Administration," Distributed and Parallel Databases, vol. 13, no. 2, pp. 135-160, 2003.

[6] Schnier B, Applied Cryptography, Jhon Wiley & Sons.2001

[7] Singh B., Network Security and Management 2nd ed. Prentice-Hall of India Pvt.Ltd., New Delhi(2009)

[8] Sudarshan .S, Korth Henry F, Silberschatz Abraham," Databases System Concept", McGraw Hill International edition .6th Edition , 2011

[9] Weippl Edgar R " IT Security Context in E-Learning," September 10,2008

[10] Weippl Edgar R. "Security in E-Learning" , Springer Publication ,2005

[11] http://www.databasesecurity.com:last accessed on 11/08/2013

[12] http://www.oreilly.com/:last accessed on 01/01/2014

[13] www.db-security.org/:last accessed on 01/01/2014

[14] http://en.wikipedia.org/wiki:last accessed on 01/01/2014

[15] http://www.imperva.com:last accessed on 01/01/2014

[16] Database Security Guide Updated November, 2009 by IBM.

[17] Kikelomo Maria Apampa "Presence verification for summative e-Assessments;"Thesis at School of Electronics And Computer Science" August 2010.

[18] http://www.itu.int/ITU-D/icteye/Indicators/ WTI_ Technotes.pdf last accessed on 26-01-2014.