IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 1 (July-Aug. 2012), PP 24-27
www.iosrjournals.org

Secured E-Learning Content on USB/HDD Device

V. Krishnamurthy, Ajinkya Deshmukh, Rupesh Rathod and Nirajsingh Yeotikar
National Institute of Electronics and Information Technology, Aurangabad Dr BAM University Campus

Abstract: *In this paper, we propose the protection to e-learning content present on USB/HDD device. Unlike a onetime classroom session, the e-learning course is available for others... Our proposed system provides the security to this content present on flash drives with the authentication, confidentiality, copy protection and authorization. Firstly user will registering for course then he will get the encrypted data on authenticated USB device. As soon as he authenticates the system, USB and himself, he will have authorized to have license file. Using it he can play the course content. We conclude that the proposed system is secured using three level authentication, confidentiality and integrity of data, copy protection and online authorization.*
Keywords: *Authentication, Authorization, Confidentiality, Encryption, Piracy Protection*

I. INTRODUCTION

In today's era one has to update oneself continuously to survive in this competitive world. E-learning is the best solution for this. Developers put lots of efforts to develop these e-learning courses to make them more interactive and interesting. To get good revenue from the course content, it must be secured from piracy as it is to make copy of the content and distribute to others.

The e-learning can be achieved online as well as offline i.e. synchronous and asynchronous learning. Synchronous learning needs continuous high speed net connection for user and larger bandwidth for the organization. In today's scenario it is not possible to own larger bandwidth. To make e-learning more effective and more interesting we need to make our content multimedia reach, resulting in the increased content size and so increased bandwidth. This is neither affordable to user who will need high speed internet all the time nor to the provider who will need larger bandwidth. So the option is Asynchronous e-learning. In asynchronous e-learning you will provide the learning content in the CD or USB.

Providing learning content through USB needs many issues to be considered. Here the security in e-learning comes. The integrity and confidentiality of learning content is the major security issue comes first. To provide the security to learning content, avoid its piracy and provide the course content only to those who are authenticated and authorized by registering and paying for the course are some security parameters of e-learning. Learning content is secured by implementing security aspects as authentication, authorization, encryption and copy protection. Authentication is done at three levels User authentication, System authentication and USB authentication. Password based AES 256 encryption algorithm is used to maintain confidentiality of data. Security algorithms are implemented in java and the hardware interfacing i.e. interfacing with USB hardware lock and user's system is done in C sharp (e.g. [1]). Interfacing of both the programming languages is achieved by using Java Native Interface. For automatic detection of insertion and removal of USB (e.g. [2]) and for applying the copy protection scheme to the system windows services is used. User registration, login creation and modular authorization is done in online security module. Modular access of user is controlled through online security module by maintain the record of user of modular access. User is provided the license file for a module only once on his registration for that module. This web application is implemented using J2EE tool, JDBC and Java auto mailing classes.

The flow of security implementation is shown in diagram

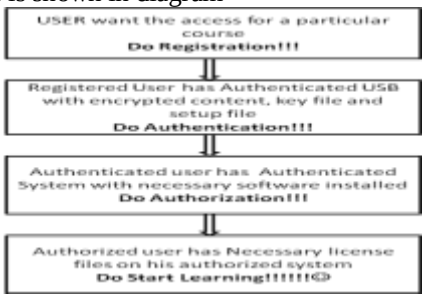

Fig. 1 Sequential steps for user

The complete system is mainly divided in two parts namely provider side and user side. The provider side includes the authentication of content provider, USB registration and its database maintenance; secure key

file and license file creation, encryption of content, setup file creation, user registration and its database handling. The user side includes the login, user authentication, user's system authentication, authorization of user and system, playing the decrypted content and maintaining the copy protection of the content.

The outline of this paper as follows: Section 2 describes the access control of data to user. Section 3 describes the data integrity and confidentiality. Section 4 describes the copy protection of data. Section 5 depicts the online security module and is followed by our conclusion in section 6.

II. ACCESS CONTROL

Access control is to permit or deny access to data. This involves authentication and authorization. Authentication is normally a prerequisite for authorization, but they are separate and distinct concepts.

- Authentication establishes who you are.
- Authorization establishes what you are allowed to do.

A. Provider Authentication

The content provider's authentication is necessary so that there will not be fake providers earning with fake brands. Authentication is necessary in order to ensure that the content in the said USB used by user is the one, provided by the original provider and is not the pirated. To achieve this USB containing the encrypted course data is authenticated. Its authenticity is checked for every access. To authenticate or to identify USB uniquely some of its hardware details are accessed.

1) Uniqueness of USB: The USB the mass storage device has some unique identity provided by its vendor. All USB devices have a hierarchy of descriptors which describe to the host information such as what the device is, who makes it, what version of USB it supports, how many ways it can be configured, the number of endpoints and their types etc. USB devices can only have one device descriptor. We used these parameters to uniquely define the USB storage device we are using to provide the course data within. The vendor id, product id and serial number of the USB are accessed using Windows Management Instrumentation (WMI) classes. The fingerprint of 16 byte is calculated using these three parameters. This fingerprint of USB is unique for it and no other USB could have the same fingerprint. It is used as one of the parameter needed for encryption and decryption of the course content. It is used by provider when he encrypts the data. At user side the content is decrypted but to decrypt the secure is needed and that can be accessed only with the unique fingerprint of the USB containing the data. So to decrypt the content the authenticated USB must be enumerated in the system. In this way by authenticating the USB with content one step of security is assured.

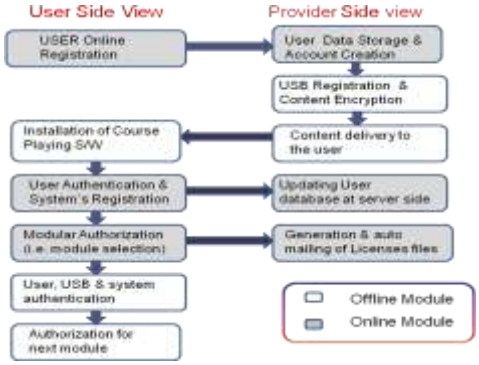

Fig. 2 Flowchart of system

B. User Authentication

User authentication is achieved with his password and the unique id of user's system.

1) User Password: This is accepted while authorization of the user which is done online. The password from user is accepted and directly used in key generation and encryption of license file. This password is neither stored in database anywhere nor hardcoded in any software. Once user is authorized for a particular module he can decrypt the related content and use it to learn. But for every access he has to enter the password. The decrypted license file is the one parameter needed to access the key file which stores secure key for decryption of the course content.

2)Unique ID of user system: The system is uniquely authenticated using its unique unalterable hardware details such as processor id, bios id, hard disk serial number, motherboard serial number. These details give uniqueness to every system. Here we are accessing these details to generate the 16byte fingerprint. This is generated at the time of setup file installation. It is queried to the user at the time of authorization and used as parameter to store key which encrypts license file. To get these hardware details for first time and for every login WMI classes and properties are used.

In this way the authenticated user has authorization to access the data on his system only. By creating unique authentication id of his system and using it as a parameter to decrypt license file is another level of security added. The same authentication id is calculated at runtime for every access and if it is same then only the license file get decrypted and that license can be used internally to access secure key file which is needed actually to decrypt the course content.

To access the WMI classes to get the hardware details we are using C#. These accessed authentication parameters are then used in encryption step to increase the security level. So to communicate between java and C#, 'Java Native Interface' (JNI) is used.

III. DATA INTEGRITY AND CONFIDENTIALITY

Data confidentiality includes data access by authenticated and authorized user. And data integrity states that data should not be tampered with or modify. The content confidentiality and integrity is achieved to some extent by encrypting the content using some hardware details of both USB and user's system (e.g. [2]). The decryption and further use of data is made possible only when user knows his password, he is using the same USB provided by course provider and his own system which is authenticated. AES cryptographic algorithm is implemented using Java cryptography Architecture (JCA) and Java Cryptography Extensions (JCE). (e.g. [3],[4])

IV. COPY PROTECTION AND COPY AVOIDANCE

A) Copy Protection

It summarizes as anyone can copy the course content from USB but he will not be able to use (read/play) it until and unless he has the same authenticated USB with him, he knows the password. In short only the authenticated user authorized by course provider can only use this content. Copy protection is achieved as for the decryption of content USB, user's authenticated system and password is must. This is achieved using the encryption and making the key access dependant on three parameters password, USB hardware details and user System hardware details. Though someone copies all the content from USB he cannot decrypt and use it till he got the above mentioned three parameters at the same time. It means he should have knowledge of secret password, system for which he got the authorization from content provider and authenticated USB enumerated in the authorized system.

B) Copy Avoidance

It means nobody can copy the data from its original position. This is necessary when authenticated user is playing courseware on his authorized system. Copy avoidance is to protect the decrypted data. The copy avoidance is achieved by avoiding the copy and/or cut action when the authenticated content USB is running. More security feature applied is if user tries to stop the copy avoidance mechanism the USB stops working and immediately gets ejected. Copy avoidance is implemented by controlling following control listed below

- Copy paste
  - Right click
  - ^c ^v
- Cut paste
  - Right click
  - ^x ^v
- Print screen
- Send to
- Drag drop

V. ONLINE SECURITY MODULE

An online security module is implemented as server client system. Online java programming is done using J2EE tool. The code is developed with JSP and JavaBeans using different API's like java security API for encryption, Java Mailing for auto mailing of license and password file to the user/client. JDBC driver connection is used to store the user data and to

Fig 4. Flowchart of overview of Online Security Module

create user account. Apache Tomcat Server has been used to deploy the online server programs. JSP, JavaBean programming are used for user registration and JDBC for storing user data into MYSQL database server. For automatic mail to the user is given by using Java Mailing API (e.g. [5]-[7]). From two flowcharts given below online security module become clear.

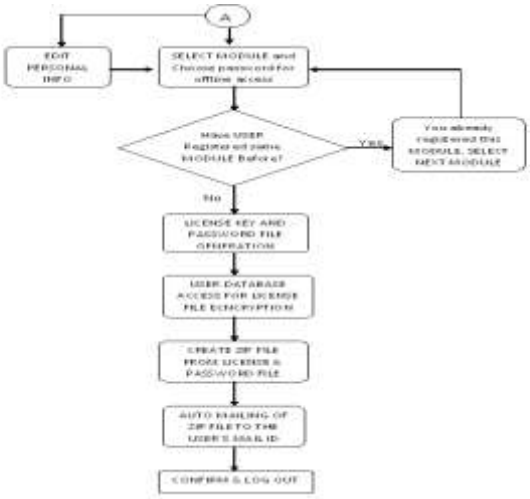

Fig 4. Flowchart of overview of Online Security Module

VI. CONCLUSION

In this paper, we propose that the E-Learning course content is secured using three level authentication user authentication, USB authentication and System authentication. Confidentiality and integrity of data is maintained using AES Encryption algorithm and piracy is avoided using copy protection and online authorization. Tracking of course activity and keeping records of modular access is done on server side. This way user can read/play the course content only with USB hardware lock and only on a system authenticated for course access. User cannot make copy of the course content for further distribution to others and hence there is increase in revenue of developer.

ACKNOWLEDGMENT

We take this opportunity to express my deep sense of gratitude and sincere thanks to Dr. V. N. Walivadekar, Rtd Director, NIELIT centre, Aurangabad. We would also thank to Mr S. T. Valunjkar, Director In-Charge, NIELIT centre, Aurangabad for continuing to provide support and motivation. We would like to thank to our project guide Mr. V. Krishnamurthy, under whose guidance, continuous encouragement and support this work was carried out. We are very much thankful to Mr. Alok Tripathi, NIELIT Centre, Gorakhpur for his guidance and valuable suggestions whenever we faced problems. We are also thankful to our seniors Ms. Rupali Mankar and Ms.Amruta Faude who have also contributed a great deal for the initial completion of the work. This work was carried out in and supported by the National Institute of Electronics and Information Technology, Aurangabad.

REFERENCES

[1] C# station. (2000). [Online]. Available: http://www.csharp-station.com/Tutorial
[2] Jan Axelson, USB Complete, 4th ed., June 2009.
[3] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197,November 26, 2001. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[4] Oracle(2003)ReferenceGuidehomepageonOracle.[Online].Available:ttp://docs.oracle.com/javase/1.4.2/docs/guide/security/jce/JCE RefGuide.html#EncrDec
[5] ScottMcPherson.(2010)JavahomepageonSDN.[Online].Available: ttp://java.sun.com/developer/technicalArticles/Programming/jsp/
[6] MySQL5.0ReferenceManual. (1997) homepage on Mysql. [Online]. Available: http://dev.mysql.com/doc/refman/5.0/en/index.html
[7] JavaMail API Documentation. (2011) homepage on Oracle. [Online]. Available: http://javamail.kenai.com/nonav/javadocs/