IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 21-26
www.iosrjournals.org

Secured E-Learning Content on Handheld Device

V. Krishnamurthy, Sushma Dakh, Kirti Bhakkad, Nilima Bargal
National Institute of Electronics and Information Technology, Aurangabad Dr. BAM University Campus ,0240-2400120

***Abstract**: To survive in this competitive world one has to update him continuously with the latest trends and new emerging technologies. It is not feasible for everyone to go and learn at different places. For this reason e-learning is a new emerging methodology of learning process. We have many such e-learning systems in existence but the e-content of those are easily prone to the piracy because of the lack of the security features in it. As online mode compels the user to use continuous internet connection for playing course, the offline solutions of such system would be more economic product for the users. In this paper we propose a system which provides security to the e-learning content deliver to users on handheld device with System Authentication, password protection, data encryption by using AES 128 bit Algorithm and piracy protection which is achieved by web-view control and managing system control. The handheld device can be connected to the television set to view the content which makes the solution very cheap and compact.*
***Keywords:** Piracy Protection, E- learning Security, Fingerprint Authentication, Data Encryption.*

I. Introduction

To survive in this competitive world one has to update oneself continuously. It is not feasible for everyone to go and learn at different places. For this reason e-learning is a new emerging methodology introduced in to make the learning process smoother and simpler. Now a day's lots of study material from reputed institutes and universities are available in e-learning course environment which are well managed, interactive and made interesting using learning management system. To get worthy return of these efforts taken by experts, the course should be available to authenticated person who has paid for it, and hence so we need to secure it from piracy.

In the field of education different categories of systems have been proposed to help students acquire knowledge and/or skills in various domains. In the very beginning, the designs of educational systems were based on the principle of teaching sets of universally valid reference knowledge in a standard way. As a consequence, a modular architecture with three main components (domain knowledge, pedagogical expertise and learner model) was developed. But the educational research has shown that it is not possible to determine a universal teaching strategy when we take into account human differences. Educational systems based on modular architectures have shown to be too rigid to deal with the quick evolution of knowledge and the diversity of human culture and cognitive styles [1].

One has to consider many factors while providing learning content through handheld device and here comes the security of e-learning in to picture. The integrity and confidentiality of learning content is the major concern that comes first. Security of content, avoid its piracy, authentication and authorization are some of the key security parameters of e-learning.

Synchronous learning needs continuous internet connection for playing course content on device. Now a day's smart devices are becoming very popular among youth. The reason behind this is its portability, compactness and cheaper rates. The same device can be connected to internet to achieve online connectivity. Using battery connectivity such device can be used for continuous learning in remote places. So the option for asynchronous e-learning having portable smart devices (smart phones and handheld devices) in affordable price takes over. But since it is easily prone to piracy, we have provided security to such Smart devices.

Earlier research in the e-learning domain has mainly focused on providing and delivering content and infrastructure. Security issues though have rarely been considered. Security is usually not taken as a central concern in most implementations either because systems are usually deployed in controlled environments, or because they take the one-to-one tutoring approach, not requiring strict security measures. Considering though the scenario of a highly interactive e-learning application constructed over heterogeneous, distributed and open architectures, the potential threats to security cannot be neglected. Previous work on secured e-learning concerns security aspect of e-learning on windows OS platform as their work is platform and device dependent [2]. We continued same work and try made it platform and device independent by implementing all codes in platform independent language and scripts.

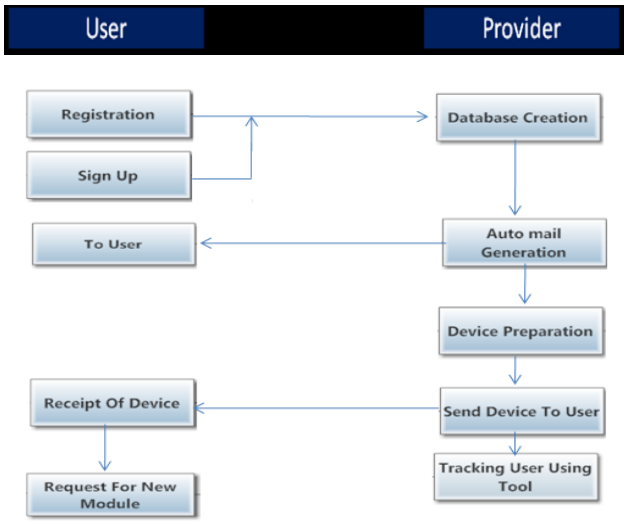

Fig. 1 Flowchart of System

II. Need Of Security Feature

The course content is the most valuable part of e-learning. The course provider puts lot of efforts and experts guidance to create efficient and best quality content so that learner should find learning effective and excellent. They have to put initial cost and man power to create content which can be regained with profit when users start accessing those contents. In between for those who want the learning with less or with no cost piracy comes forward.

The tendency of people to gain more out of less or nothing has corrupted the whole system. The hackers, intruders or unauthenticated people access those learning content illegally, create the pirated copies and sell them at low cost. Use of e-learning content offline needs many issues to be considered. Here comes the security for e-content in to picture.

Security is achieved with the implementation of following parameters,

- User Registration Module
- Payment Gateway Module
- Authentication Module
- Play Module

III. Security Method For Data Security

As described in previous sections, it is an important to secure e-contents from piracy. In our system we implemented a module called an authentication agent module which detect authentication parameters, these parameters can be generated using two modes

- Online Mode
- Offline Mode
-

3.1 Online mode

In this mode uses IP Address, MAC address, storage identification, processor identification and device model no are accessed. If end user tries to change an IP address using third party (such as proxy servers) tool this mode will detect it and assigned as unauthenticated user.

3.2 Offline mode

This mode uses only physical details such as OS ID and device ID model information and generate 16 byte key. This key is stored in database server and used for encryption of modules by AES 128 algorithm.

Cryptography is the biggest tool in the application programmer's weapon store. But it is important to realize that a cryptographically enabled program is not necessarily a secure one, without a carefully planned and constantly scrutinized security strategy. Correctly used, cryptography provides following standard security features:

- Confidentiality assures you that data cannot be viewed by unauthorized people.
- Integrity assures you that data has not been changed without your knowledge.
- Authentication assures you that people you deal with are not imposters.

- Authorization provides the access control to the authenticated user.
- Privacy protection assures the copy protection of your data.

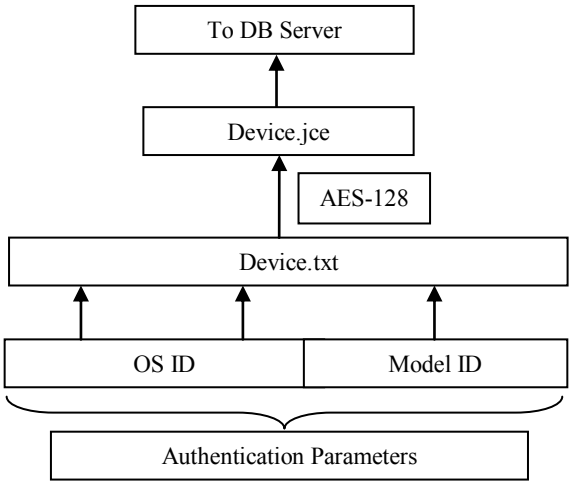

Fig. 2 Authentication Agent

According to this standard feature of cryptography we will generate installation key using AES 128 Algorithm and Authentication parameters which can be online or offline mode.

3.3 AES 128 Algorithm

The AES algorithm consists of ten rounds of encryption. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption. After an initial round, during which the first round key is XORed to the plain text (Addroundkey operation), nine equally structured rounds follow. Each round consists of the following operations:

- Substitute bytes
- Shift rows Mix
- Columns Add
- Round key

The tenth round is similar to rounds one to nine, but the Mix columns step is omitted [3].

IV. Methodology And Tools

E-Learning content is secured by implementing security aspects such as authentication, authorization, encryption and copy protection.

To implement the client and server side application system we use different techniques and highly ended tools(RAD-Rapid Application Development) .We implement system with Four different modules they are:

- User Registration Module
- Payment Gateway Module
- Authentication Module
- Play Module
-

4.1 User registration module

This is the first Interaction of Client and server, to implement the registration module we used these different web components:

- Client Side Scripting
- Server Side Scripting
- Database Server Language
- Protocol to communicate

4.1.1 Client side scripting

Scripting is nothing but a small program to validate given information from end user [5]. This information can be check in server side but server having many different responsibilities. Client Side Scripting can be run in markup language and different style (for android Tab) to run static web pages.

4.1.2. Server side scripting

In web some time we need web application to generate web pages according to user specification such as Administrator can perform operation on module and Client can only download module. For all users we implement dynamic web page using servlet and jsp technology. We used java server programming in such area which interact with user interface layer and business logic layer and generate dynamic page with less code more output.

4.2 Payment gateway module

It is the most critical module in this system, this module is used to manage client payment and gives an acknowledgement of payment receive, after giving acknowledgement of payment gateway web server will store it in database server and after that user will enable to download particular module according request.

4.3 Authentication module

Authentication module is basically divided into two agents they are:

4.3.1 Authentication agent about this agent we already discuss in previous sections

4.3.2. Verification agent will verify password and fetch system details and generate 16 byte key for authentication.

If the system is authenticated one then decryption key(.jce) and generated key (.jce) are same and module will decrypted. And all these performed silently in background like services[6].

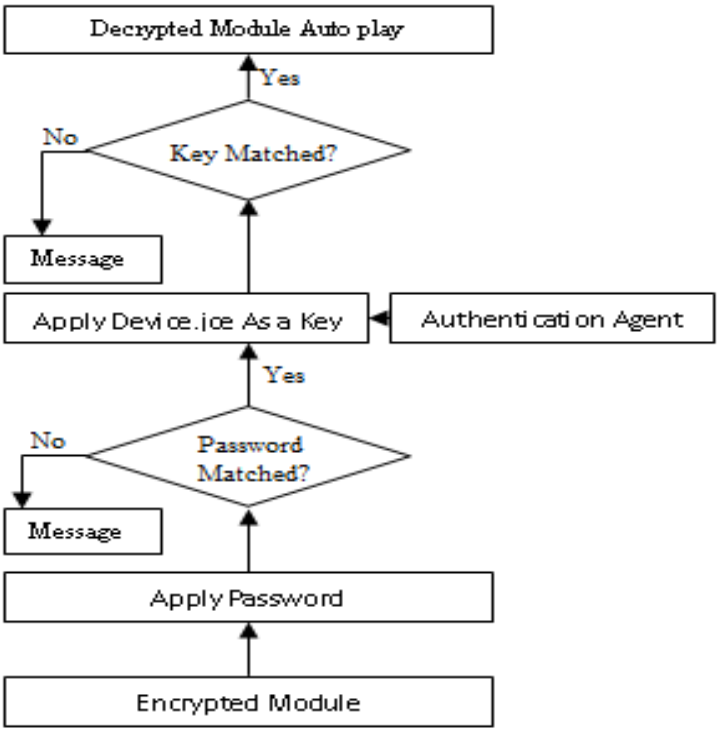

Figure 3. Verification Agents

4.4 Play module

After completing two level authentications the play module will start two modules using multithreading concept these modules are timer and piracy protection mechanism.

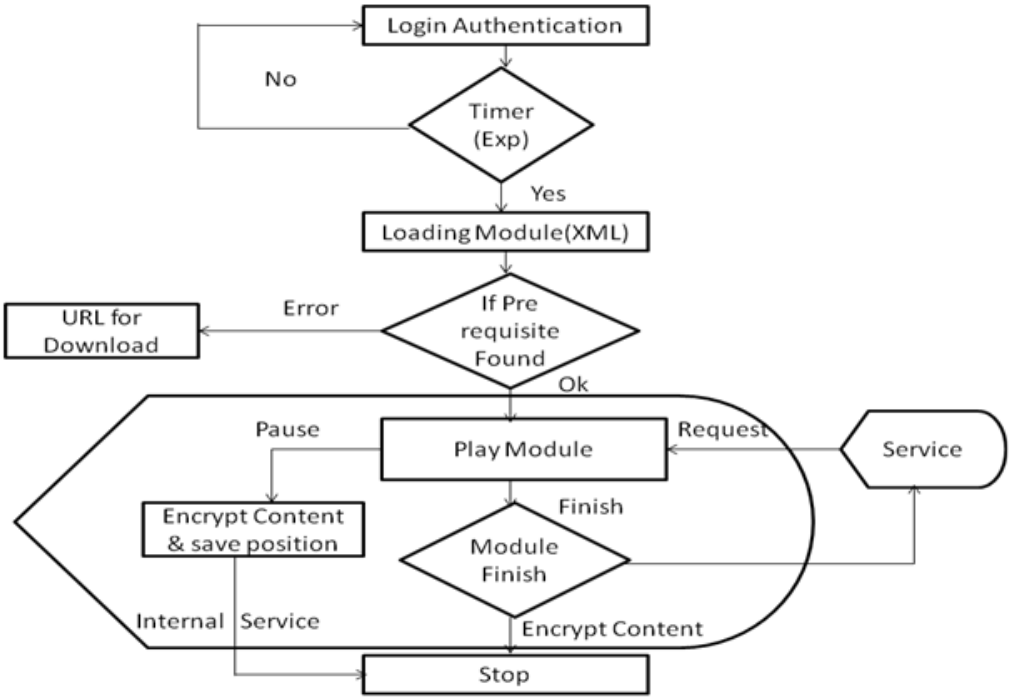

Figure 4. Play Module

After the successful authentication, timer control is initiated if session is still live else user will have to login again in case timer session has timed out. This timer thread will continuously generate tick count to load the module. And once the module is successfully loaded, prerequisites are checked whether they are present or not if available then run the module. In case, if something is missing, user will be redirected to URL for downloading the required prerequisite. Once this check is passed, module will be open the file in full screen mode using web view control in android and continuously clear system clipboard area to protect system and finally user can enjoy that session. In case of any interrupts (like incoming call, system interrupt) it will halt the processing and stop timer thread and switch to particular task. After completion that task user can either resume that content and continue with it or stop the system.

When user stops the system it will stop the time count and store the data in SQLite DB in encrypted format and disable all piracy protection mechanism.

V. Database Design

5.1 Database server language

To interact with database server we need database language such as ANSI Structured Query Language which can be run anywhere in database management system. And for transaction and other activities of database server we use oracle enterprise edition which can hold huge amount of data. This transaction will be done using JDBC bridge technology and oracle thin driver.

Data storage in Client Side data storage options are the following:

- Shared Preferences Store- private primitive data in key-value pairs.
- Internal Storage- Store private data on the device memory.
- External Storage- Store public data on the shared external storage.
- SQLite Databases- Store structured data in a private database.
- Network Connection- Store data on the web with your own network server.

At the time of database design on server side we should keep in mind [5]

- How to reduce data duplications in Android system and database server.
- Concept of Denormalization in Database and how we normalize our database.
- We need to use technique called data Integrity.
- Design a database which Controls an e-contents in secure manner.

5.2 Protocol to communicate

Web system can communicate using protocol such as http, https and FTP protocols. We use http for general request response context, https we use at the time of payment gateway in PayPal system and ftp used to transfer e-contents after all verification done.

VI. Conclusion

In this paper, we have given Secured E-Learning On Handheld Device that eliminates basic overheads of conventional learning approach. e-content is secured using two level authentication user authentication, system authentication. User can only access the e-content on authenticated system. Confidentiality and integrity of data is maintained using AES-128 encryption algorithm and piracy is avoided using piracy protection mechanism and offline authorization. This way user can read/play the course content only with password and on authenticated system. Cannot copy the course content for further distribution or if any way it happens User cannot play content on unauthenticated system.

Acknowledgment

We take this opportunity to express our deep sense of gratitude and sincere thanks to Mr S. T. Valunjkar, Director In-Charge, NIELIT centre, Aurangabad. We would like to thank our project guide Mr.V.Krishnamurthy, under whose guidance, continuous encouragement and support this work was carried out. We are very thankful to Mr. Alok Tripathi, NIELIT Centre, Gorakhpur for his guidance and valuable suggestions whenever we faced problems. We would also like to thank Mr. Sayed Mujahed Hussaini, NIELIT centre, Aurangabad for continuing to provide support and motivation. We are also very thankful for valuable work of Rupali Mankar, Amruta Fawde, Rupesh Rathod, Ajinkya Deshmukh and Niraj Yeotikar who created a firm platform for us. This work was supported by the National Institute of Electronics and Information Technology, Aurangabad.

References

[1] N. Balacheff, "A modelling challenge: untangling learners' knowing", in Journées Internationales d'Orsay sur les Sciences Cognitives: L'apprentissage, JIOSC2000: Paris,2000

[2] V. Krishnamurthy, Ajinkya Deshmukh, Rupesh Rathod and Nirajsingh Yeotikar, Secured E-Learning Content on USB/HDD Device,IOSR, Volume 3, Issue 1 (July-Aug. 2012)

[3] M. Pitchaiah, Philemon Daniel Praveen, Implementation AES Algorithm, IJSER Volume ,Iissue 3 (March 2012).

[4] Yadav, Subhash Chandra, Singh, Sanjay Kumar, An Introduction to Client/Server Computing, New Age International Publication, 2009-03

[5] Sam R. Alapati, Charles Kim, Oracle Database 11g, Apress, 2007.

[6] V. Krishnamurthy, Pravin Gade, Practical Implementation of Secured E-Learning with Cryptographic Approach on Android Smart Devices,IJERT, Volume 2, Issue 7 (July 2013)