Practical Implementation Of Secured E-Learning With Cryptographic Approach On Android Smart Devices

V. Krishnamurthy
National Institute of Electronics and Information Technology, Aurangabad
Dr. BAM University Campus,

Pravin Gade
National Institute of Electronics and Information Technology, Aurangabad
Dr. BAM University Campus,

Abstract

In existing e-learning environment e-contents are easily prone to the piracy because lack of the security features in the environment. In the last decade smart devices (smart phone or tab) are often used with different android OS. In this paper, we implemented Security for the e-learning Contents by using System Authentication, password protection, data encryption by using AES 128 bit Algorithm and piracy protection to e-learning content delivered to user on his smart device achieved by web view control and managing system controls.

1. Introduction

At the dawn of the new millennium, e-learning is increasingly viewed as a competitive weapon. Business success depends largely on high-quality employee performance, which in turn necessitates high-quality training. In the quest to remain competitive in today's hyper-competitive market is exploiting technology revolution in order to train more rapidly, efficiently, and cost effectively. Exponential growth of the internet provides the ideal delivery vehicle for education.

Through its increasing reach and simplicity of use, the internet has paved the way for a global learning community to exist where language and geographic barriers to education have been erased. The new knowledge economy puts a premium on intellectual capital making lifelong education more important than ever. However, the education constraints are becoming more prevalent. Accordingly, e-leaning is a vital asset for all in the new knowledge economy.

Synchronous learning needs continuous internet connection for playing course content on device So the option for Asynchronous e-learning is to have smart device (smart phone or tablet PC) which is affordable and portable . 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. But asynchronous e-learning easily prone to piracy. We provided security to these e-learning content on Smart devices to reduce piracy.

Previous 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'[1] concerns security aspect of e-learning on windows OS platform as their work is platform dependent as well device dependent. We continued same work and try made it platform and device independent by implementing all codes in platform independent language and scripts.

2. Need of security features

The e-learning content is the most valuable part of e-learning. The course provider institutes put lot much efforts and experts guidance as well as hard work 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 and then that 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, how learning will remain unaffected? 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 the security for e-content comes in to picture. 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. So security is achieved with the implementation of following parameters

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

3. System objectives

The complete system is mainly divided in two parts namely provider side and user side. The provider side includes the authentication of content, registration and its database maintenance, encryption of content, setup file creation, user registration and its database handling. And the user side includes the login, user authentication, user's device authentication, decryption of e-content, playing the decrypted content, Tracking course duration and maintaining the piracy protection of the content[1].

4. Database storage & design

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[2]

- 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. Security mechanisms for securing data

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

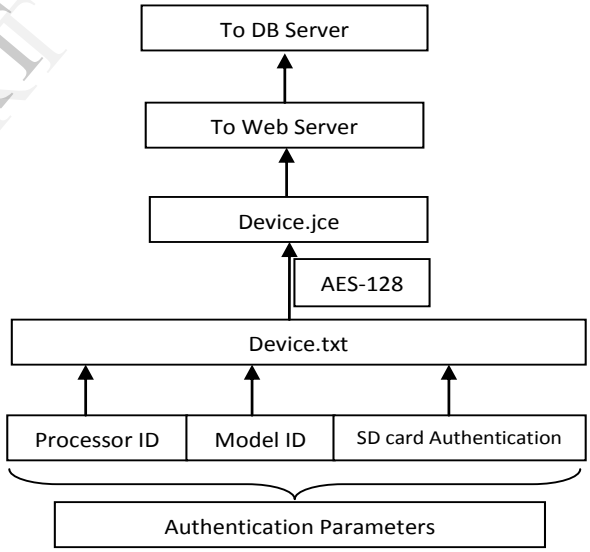

Figure 1. Authentication Agent

- Online Mode
- Offline Mode

1.1. Online mode

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.

1.2. Offline mode

This mode uses only physical details such as storage id, processor id and device model information and generate 16 byte key, send it to web server. This key is stored in database server and used foe 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 these 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.

And 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.

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 rowsMix
- columnsAdd
- round key

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

6. 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

6.1. 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

6.1.1 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.

6.1.2. 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.

Some time we need to perform a transaction and that should be covered in respect to time for that reason we use servlet technology which will not covert web page into servlet and eliminate conversion step[5].

6.1.3. 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 done using JDBC bridge technology and oracle thin driver.

6.1.4. 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.

6.2. 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.

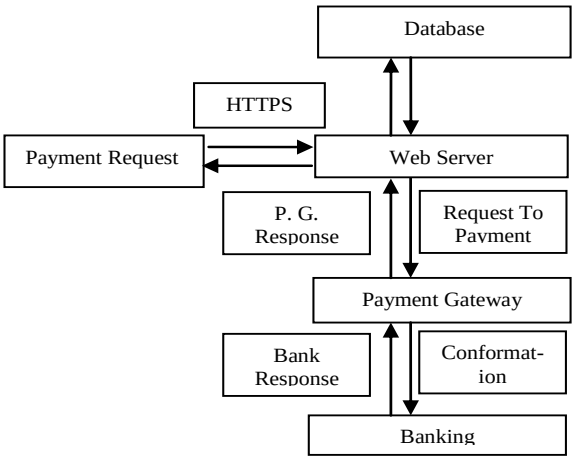

Figure 1. Payment Gateway Module

6.3. Authentication module

Authentication module is basically divided into two agents they are:

6.3.1. Authentication agent About this agent we already discuss in previous sections

6.3.2. Verification agent will verify password and fetch system details and generate 16 byte key for authentication. And if the system is authenticated one then decryption key(.jce) and generated key(.jce) is same and module will decrypted. And all these activities after password verification perform silently in background like services.

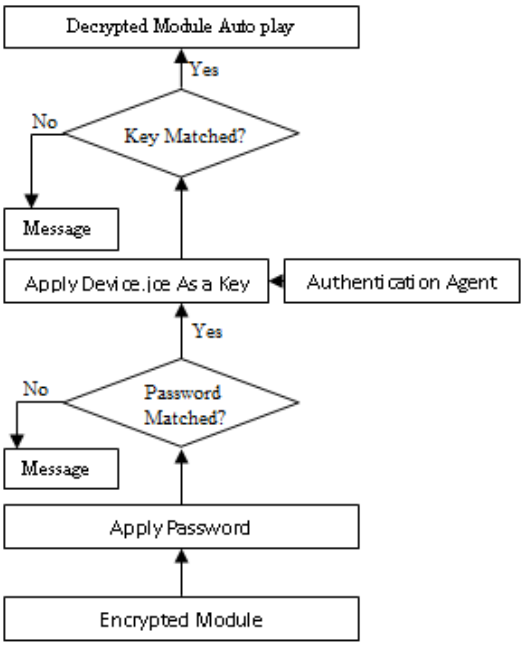

Figure 1. Verification Agents

6.4. 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.

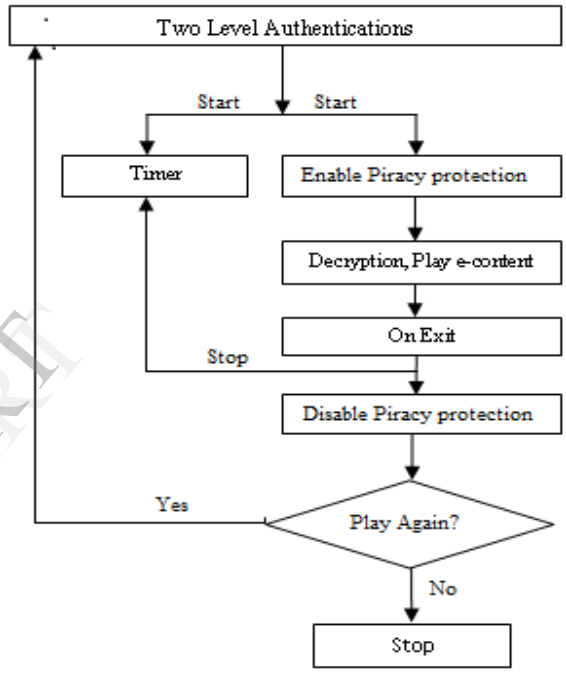

Figure 1. Play Module

Timer thread will continuously generate tick count and specify the usage of module.

Piracy protection mechanism will open that e-content 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 but if some interrupts (like incoming call, system interrupt) generates that time play module will halt the processing and stop timer thread and switch to particular task and after completion that task user can resume that content and continue with it or stop the system. When user stop the system at that time it stop time count first and store it in SQLite database and also disable all piracy protection mechanism.

7. Conclusion

In this paper, we have given practical implementation of secured e-learning with cryptographic approach on android devices 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.

8. Acknowledgments

We take this opportunity to express our deep sense of gratitude and sincere thanks to Dr. V. N. Walivadekar, Rtd Director, NIELIT Centre, Aurangabad. We would also like to thank Mr. S. T. Valunjkar, Director In-Charge, NIELIT centre, Aurangabad for continuing to provide support and motivation. We are very thankful to Mr. Alok Tripathi, NIELIT Centre, Gorakhpur for his guidance and valuable suggestions whenever we faced problems. We are also very thankful for valuable work of Rupali Mankar, Amruta Phawde, 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.

9. References

[1] 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)

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

[3] M. Pitchaiah, Philemon Daniel Praveen, Implementation AES Algorithm, IJSER vol 3 issue 3 march 2012.

[4] Jonathan Simon, Head First Android Development, O'Reilly Media, 2012.

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