ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 48

9th International Economics, Management and Education Technology Conference (IEMETC 2017)

Construction and Technology Research of Mobile Learning System for Intelligent Devices

Xiaoxing Ma

Tianjin Hexi District Zhujiang Road 25# TianjinUniversity of Finance & Economics, 300222, Tianjin

[a]xxingl@163.com

Keywords: Intelligent devices. Mobile Learning System. DRM. Distance education.

Abstract. In recent years, the rapid development of a distance learning turn into a new force. As a new carrier, education based on intelligent devices refers to the learners take curriculum through intelligent devices, learners are no longer restrict to specific learning sites and computers, but have more free to choose their favorite course for education at anytime and anywhere. In this paper, we study the construction and the key technology for the mobile learning system for intelligent devices.

Introduction

With the advent of the Internet era, distance education has undergone profound changes, along with the widespread use of intelligent mobile devices, learners are no longer restrict to specific learning sites and computers, but have more free to choose their favorite course for study at anytime and anywhere. Through the whole learning process, learners, lecturers [4], research and development staff are in a moving process.

Intelligent devices are easy to carry, in recent years, the rapid development of a distance learning turn into a new force. As a new carrier, curriculum based on intelligent devices refers to the learners take curriculum through intelligent devices, this is a typical, personalized learning methods, and promote the pace of building a learning society in China [1]. Compared with the traditional learning, the mobile learning system of intelligent devices has the characteristics: mobility of learning environment, convenience of access, fragmentation of content, individualization of learning, timeliness of communication and practicality of purpose.

Features of Mobile Learning Systems based on Intelligent Devices

The Mobility for Learning Time and Place. In the mobile Internet era, learners use mobile phones [2], tablets and other easy to carry mobile terminals. Learners use their devices to study, do not have constraints from the time, and they can learn at any place: Campus, home, parks, shopping malls, trains, airplanes, public transport and other transport facilities. The four elements involved in teaching (students, teachers, teaching media, teaching content) are in a state of move, learners are no longer subject to the computer, you can learn anytime, anywhere. Learning is no longer subject to the time and place of former Internet era of distance education, can give learners more free of learning space.

Fragmentation for The Learning Process and Content. As the learning devices has the functions of communication, and learning places has the characteristics of mobile, learners are easy to be distracted by the external environment, resulting in the decline of learning efforts. Only the learning full of depth can form complete knowledge ability, therefore, intelligent devices learning system require the content is concise through a high degree of the content [3-4], has strong condensed structure of the knowledge, with outstanding expression of the teaching, vivid and humorous.

Timely on Learning Exchange and Interaction. Under the mobile Internet technology, geospatial constraints are greatly eliminated, the distance between teaching and learning is greatly shortened, the learning process is a dynamic interactive process, and people can communicate ideas with other people by upload audio, images and other forms of media at any time during the

learning. For the mobile Internet technology, the core features of mobile education system are happy learning, people can study at their best time and place. Of course, the interaction between teachers and students will abandon the traditional education module for distance education for the rigid interactive interaction timely between teachers and students through mobile technology. The relationship between teachers and students becomes more and more easygoing because of this interactive way of communication [1], can establish enhance friendship within and outside the classroom. When the learning pattern is embedded in the essence of life, the pleasure of learning follows.

Customized Learning Style. In the mobile Internet technology, the content of mobile learning system can be customization, according to personalized needs to develop individual learning program. In the learning methods, learning content and learning progress all have strong personality characteristics, to meet the individual's needs of learners. And in this cultural and ecological model, the learners can find the customary learning methods to meet their own characteristics due to the differences in age, knowledge structure and ability [4]. In the customized learning model, learners can make appropriate adjustments with the changes in the situation, which is other learning models cannot have.

Community Learning Object. Mobile Internet technology transforms the mobile learning platform into a "mobile Internet community" through a collaborative approach to knowledge, an open digital distance learning community attracts the widest range of learners, under the socialization of learning objects and process, social sharing is a new mode of mobile reading with content as the core and social relations as a link, focusing on sharing, communication and interaction. In socialized reading applications, through the close relation between reading platform and social networking sites, let users can share their favorite content to be synchronized in the sharing platform. Learning object of community enhance the viscous of user's under the distance education sticky, and enhance its community identity and cultural identity of the education platform.

Key Technology Research

SMS Code Verification. Illegal member use the robot program to automatically accomplish the registration, login, malicious vote, send spam messages. In this case, the verification code emerges as the times require. The verification code technology is simple, easy to implement, amount of data transmission is small, many websites using the verification code technology to distinguish between the robot and the real person, in order to enhance the safety of the website to reduce security problems. Send a verification code via SMS, is the most common and secure way to verify the true identity of the user.

SMS verification code is widely used in user registration, password recovery, login protection, identity authentication, transaction confirmation and other application scenarios. Second, the use of SMS verification code improve security of the user account effectively, is an indispensable part of e-commerce, O2O industry. High-quality SMS verification code have an irreplaceable role to enhance the user experience. At the same time, through SMS verification code, merchants will be more convenient access and interact to user information. If people register a platform do need to enter the SMS verification code, business platform will encounter different spammer attacks, costs for operating and maintenance will be greatly increased, will greatly reduce the efficiency of mobile Internet. The magnitude of the impact of junk mail is difficult to predict. For the website platform, the server resources are limited, if someone try to malicious landing, or use software to send spam, will lead to server paralysis, and ultimately drag the platform.

Encrypted Storage of Teaching Video Files. EFS (Encrypting File System), is a unique function of Windows, operating system encrypt to NTFS format for save the file and data directly, to improve the security of the data. Encryption and decryption of EFS are transparent for completion, if the user encrypted some of the data, then the authorized users' access to these data is complete permission, and other unauthorized users attempt to access the encrypted data, they will receive a error message with "no access". Encrypted files are accessible only to authorized users by

default, if there is need to share users' own encrypted files with others users on special condition, authorized users need to complete additional settings, and the share operation will only be available for individual files and not for the entire folder [5].

EFS is a public key encryption, when using EFS to encrypt a file or folder, the system first generates a FEK (File Encryption Key) consisting of pseudo-random numbers, then creates an encrypted file using FEK and the Data Extension Standard X algorithm, and store it on the hard disk, deleted the unencrypted original file simultaneously. The operation system encrypts the FEK with the public key and stores the encrypted FEK in the same encrypted file. When operation system access the encrypted file, first use the current user's private key to decrypt the FEK, and then use FEK to decrypt the file [3].

When EFS is used for the first time, the key is generated first and then encrypt the file. File encryption and decryption need the key to participate in, and the key is divided into public and private key. When encrypt the file using the public key, when decrypting the file using the corresponding private key [3] [6].

Copyright Protection of Video Files. Protection for video file copyright means encrypt the course video store in local cache, protect the users' account and key information. The DRM technology is to encrypt the digital content as the core of data encryption and anti-copy, only the authorized users can get the key for decryption, and the key can be binding with the user's hardware information. Encryption technology coupled with hardware binding technology to prevent illegal copying, this technology can achieve the purpose of copyright protection effectively.

Digital Rights Management (DRM) apply technology related to encryption, information security to protect and manage digital files such as video, audio, images, electronic documents, software and other copyright information. Specifically, the operation system establish a spreadsheet to record the copyright information and the owner of the file, according to the information, apply related technology to record, track, control the use of digital files. The digital files itself is also encrypted, only can be decryption when all sides such as manufacturers, distributors and creators to reach agreements [7].

The basic principles of DRM are simple, flexible and open. DRM is a system engineering that involves aspects technical, legal and commercial. It provides a complete set of means for the commercial operation of digital media. The emergence of DRM, so that copyright owners do not have to spend a lot of time and effort to negotiate with customers to ensure that digital media content can be legally used. DRM enables content providers to provide more content from platforms like Internet, streaming and interactive digital televisions and take a more flexible marketing method, protect their intellectual property interests simultaneously. DRM is not just protection for copyright, but also provides a complete set of solutions for the transmission, management and distribution of digital media content, so DRM is a system concept that includes the forth putting information of digital rights, distribution and management of copyrighted digital media content. Streaming media DRM mainly Microsoft Windows Media DRM, Real DRM and so on. Digital copyright protection technology can effectively eliminate the illegal copying, copying and transmission of digital information products through the network and the computer [8].

DRM for streaming media mainly is Microsoft Windows Media DRM, Real DRM and so on. Protection technology of digital copyright can effectively eliminate the illegal copying and transmission of digital information products through the network and the computer. Software for DRM server is an end to end management system for digital rights that implements an extensible platform for securely distributing digital products. Its core technology is cryptography, and the system framework is combined with specific applications, such as MPEG4 related applications [9].

The DRM technique works by building a digital program authorization center first. The coded digital program compress contents for encryption and protection by key, and the header of encrypted digital contents stores the Key ID of the URL of the program authorization center. When the user is in on-demand according to the Key ID and URL information of the contents head, the relevant key decryption can be sent out by the authorization of the digital program authorization center, and the contents can be played. The contents that needs to be protected is encrypted, and

even if it is downloaded and saved by the user, it cannot be played without the authorization of the digital program authorization center, thus protecting the copyright of the contents. In the practical DRM utilize the asymmetric encryption algorithm to encrypt the content and secure database to storage. The encryption algorithm is used for content encryption and certificate issuance: the certificate apply the public key algorithm to encrypted before deliver, encryption algorithm for content encryption will not increase the source content length.

The Encryption Algorithm and the Cipher Text Conversion Algorithm. The encryption algorithm apply in DRM has four kinds of AES algorithm, DES algorithm,3DES algorithm and a specific file encryption algorithm.

(1) DES algorithm: DES called Data Encryption Standard, is a key encryption using the block algorithm, inlet parameter for DES algorithm are three: key, data, mode. Where the key is 7 bytes total of 56 bits, is the DES algorithm work key; Data is 8 bytes total of 64 bits, is the data to be encrypted or decrypted; there are two mode for DES work: encryption Or decrypted.

(2) 3DES algorithm: 3DES (or Triple DES) is the generic for block password encryption algorithm (TDEA, Triple Data Encryption Algorithm). It is equivalent to apply a DES encryption algorithm three times for each data block. As a result of increased computing power of the computer, the length of the key for original DES password cracked by violence becomes easily; 3DES is designed to provide a relatively simple way to avoid similar attacks by increasing the length of the key for DES instead of designing a new block cipher algorithm.

(3) AES algorithm: Advanced Encryption Standard also known as Rijndael cipher, is a block encryption standard the US federal government adopted. This standard is used to replace the original DES, has been multi-analysis and widely used in the world. Unlike the DES, AES uses a substitution-permutation network architecture rather than a Feistel architecture.AES can quickly encryption-decryption in the software and hardware, easy to implement relatively, and only need very little space in storage.

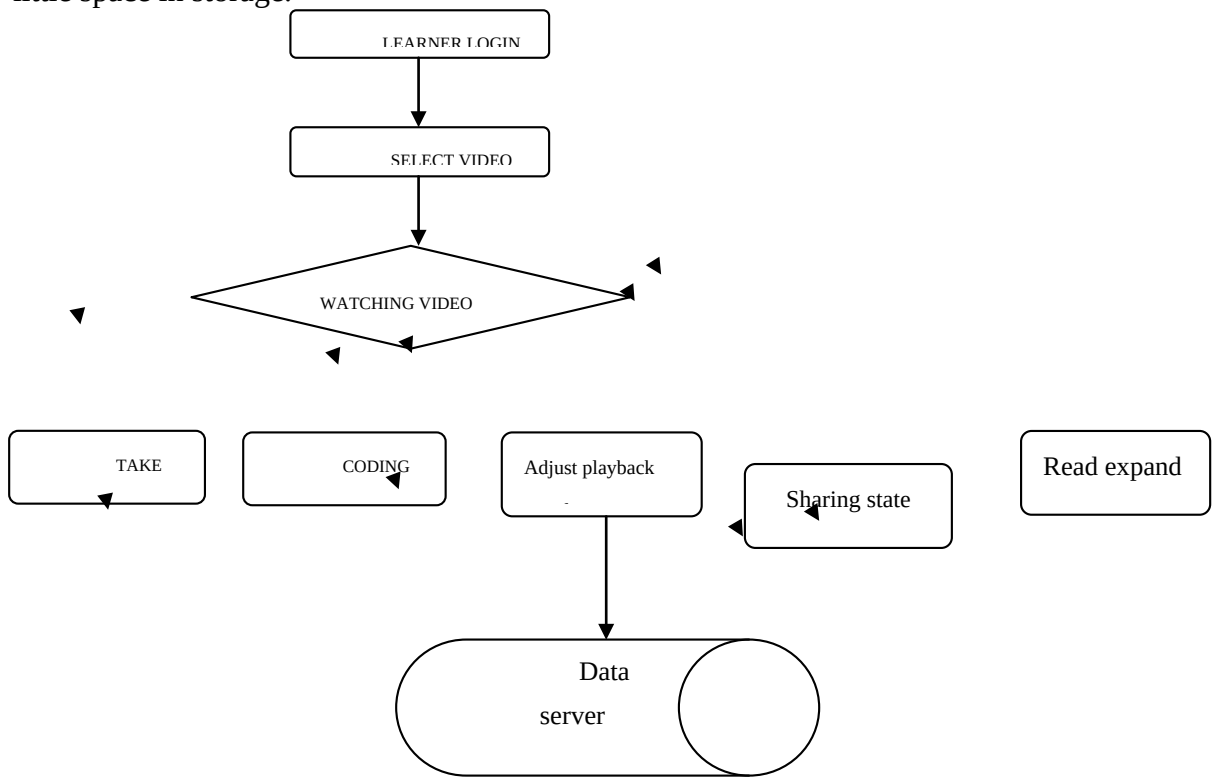

Fig.1 Business process diagram

Implementation

The main business process of mobile learning system is shown in Figure 1, we will be discuss in following areas to:

(1) The mobile learning system take the phone verification code mechanism when learner login.

(2) After login, the learner can select course video in the course video file library according to their needs. The course playback system has a pause, adjust the playback speed and other functions, the learner also can knock code, write notes and sharing learning status after pause video.

(3) The curriculum videos can be cached in the mobile learning system for learner to study at any time.

Summary

Mobile devices such as mobile phone has become a necessity for life, in the mobile Internet technology under the life of the Smartphone almost control all free time, most people gradually become "Smartphone addicts" [9], face to face of communication opportunities for between each other is reduced. The most important feature of course learning based on mobile devices is its uncertainty for learning time and space, learners are different with students from the classroom, library and other formal learning places, and learners often in a state of flow, lack of the overall learning atmosphere. This is perhaps the difference between mobile learning and traditional education in mobile Internet technology. Therefore, we should use the mobile Internet technology to develop mobile-based education, in this case, we need to optimize communicate function online in the future to increase the effective communication and promotion [7].

References

[1] WANG Meng-ru, WANG Xiao-gen, CHEN Xin-ji. Study on Design Framework of Mobile Learning System [J]. China Distance Education. 2013 (08).

[2] NIE Li-sheng. Study on Mobile Learning System Supported by 3G Communication Technology [J]. Software Journal. 2013 (11).

[3] LIU Ai-jun, LIU Zhu-qing, CHU Chu-ang.Study on Acceptance and Influencing Factors of Mobile Learning - Based on the Survey of Nanjing [J]. Open Education Research. 2013 (04).

[4] Meng Yanyue, Shi Yiping, Dong Zhijheng. Development of Mobile Learning System Based on Android [J]. Fujian computer, 2017 (3).

[5] Li Wangxiu, Li Huaxin. Construction of Digital Media Technology Course System Based on Core Competence[J]. Education Exploration, 2016 (2).

[6] ZHANG Yong-gang. Development and Security of Mobile Learning Terminal Platform Based on Android System[J]. Network Security Technology and Application , 2016 (9).

[7] Xu Liang, Ren Xiaofang, Li Xin. Based on the Android platform for mobile learning system research and development[J]. Computer knowledge and technology: academic exchange, 2016 (2).

[8] Song Chengji, Chen Xiaojian, Wang Jin. Design and Implementation of Mobile Internet Online Learning System Based on Mobile Internet[J]. Automation Technology and Applications,2017(05).

[9] Geng Qian. Mobile Learning and Playing System in PHP Course Practice[J]. Shandong Industrial Technology, 2017(05).