ATLANTIS PRESS

*Advances in Economics, Business and Management Research, volume 31*

4th International Conference on Management Science and Management Innovation (MSMI 2017)

# Design and Implementation of Secure Distributed Examination System

Yi ZHANG
School of Computer and Information Technology
Beijing Jiaotong University
Beijing, China
e-mail: 16120458@bjtu.edu.cn

Weidong ZHU
Information Technology Center
Beijing Jiaotong University
Beijing, China
e-mail: wdzhu@bjtu.edu.cn

***Abstract*—The distributed examination system based on the separation of examination sites separates the examination sites from the examination center. Examination sites are also separated from each other. The examination center's program files that are responsible for the personnel management, exam database management, randomly generating papers and assigning papers are deployed on the central server in an office. The codes of examination sites can be deployed on any PC to be in charge of downloading exam papers, examination management, marking the papers and uploading exam results. The communication between the examination center and the examination sites is carried out via the Internet. In this paper, we research the security of the distributed examination system and implement a secure distributed examination system which can guarantee a safe communication between the examination center and examination sites by means of Internet security, such as identity authentication, data encryption and data integrity authentication.**

***Keywords-distributed examination system; data encryption; identity authentication; data integrity authentication***

## I. INTRODUCTION

The traditional online examination system can not give a good response to a large-scale examination task due to the existence of defects in the structural design and implementation [1]. In the case of the number of candidates being numerous, the system prone to block and crash. The distributed examination system is designed to solve the bottleneck problem that the traditional examination system has met in large-scale examination tasks. Designing a distributed examination system based on separation of examination sites, breaks down the pressure on the examination center through scattering large-scale candidates to each examination site to identity authentication and exam.

In exam process, we need to ensure that the connection between examination center and examination sites is safe. (1) Identity authentication. Only by confirming their identity can examination center and sites carry out communication with each other. (2) Data encryption. The data transmitted in the network must be encrypted. To prevent illegal users from stealing test information. (3) Data integrity certification. The examination sites are required to inspect the integrity of the information of the exam after they receiving the exam paper package which is download from examination center to prevent data being lost or tempered. In this paper, we study the security of the distributed examination system which we design and implement then. We improve the system's concurrent access ability while ensuring the safe transmission of system data, and improve the security of the system.

## II. RELATED WORK

The system is on the base of the MVC model and puts it into effect by using J2EE framework. MVC achieves the separation of functional modules and display modules. J2EE platform is composed of a set of services, application programming interfaces and protocols that provide functional support for the development of Web-based complex applications [2].

In the process of identity authentication between examination center and the examination sites , we use the public key encryption algorithm to complete the certification. Examination sites use the public key from examination center to encrypt their own information. Examination center uses its own private key to decrypt the data and gets the information of examination sites to verify the identity of the examination sites [3].

The function of the message digests process in data integrity certification is required to meet the following characteristics [4]: (1) Given the plain text P, it is easy to calculate Hash (P). (2) Given MD(P), it is impossible to find P. (3) Given P, no one can find the P' of MD(P') = MD(P). (4) In the plain text, even if only one bit changes in input, it will lead to a completely different output. In this paper, the MD5 algorithm is used to summarize the message digest.

In addition, the encryption of sensitive data in the distributed examination system is realized by studying the principle and process of encryption algorithm such as DES, AES and RSA.

## III. SYSTEM DESIGN

### *A. The Architecture of the System*

Most of the traditional exam system is based on one examination center. All candidates log on the examination center for exam. This system structure has a big flaw. It may lead to the central server overwhelming and crashing when large-scale candidates at the same time log on the system.

The network architecture of the distributed examination system is shown in Fig. 1. The system uses a two-level server architecture, and it is composed of an examination center and multiple examination sites. The examination center is set as a primary server, and the examination sites

are set as secondary servers. Examination center generates a exam paper package. Then examination sites will download the exam package through the Internet and distribute exam paper to the candidates. Of course, we must do identity authentication before download paper.

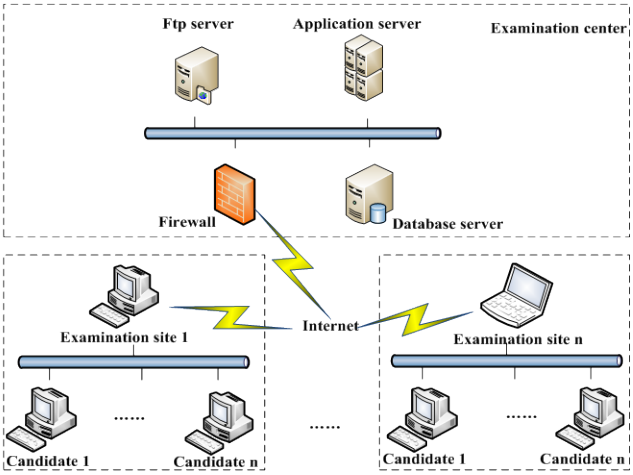


Figure 1. Distributed examination system network architecture

The design of this distributed examination system's structure is according to the idea about separating examination sites. The purpose is to spread the pressure which is in the examination center to the various examination sites. Thus it can avoid the network congestion caused by many users.

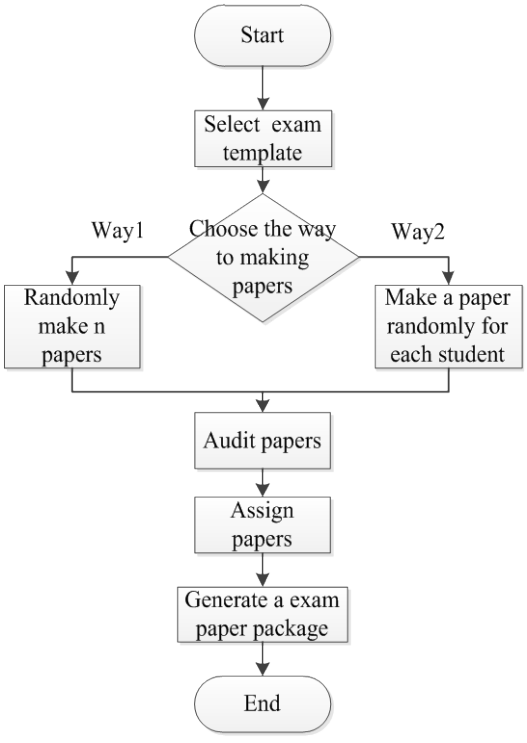


Figure 2. Examination center work flow diagram

## B. *Examination Center*

The workflow of the examination center is shown in Fig. 2. After the user verifying the identity, he logs on the examination center and obtains the exam template. Then he selects the template and the way of making papers to generate exam papers for each student randomly. After the exam papers being checked, we compress the exam information and the final exam package is generated.

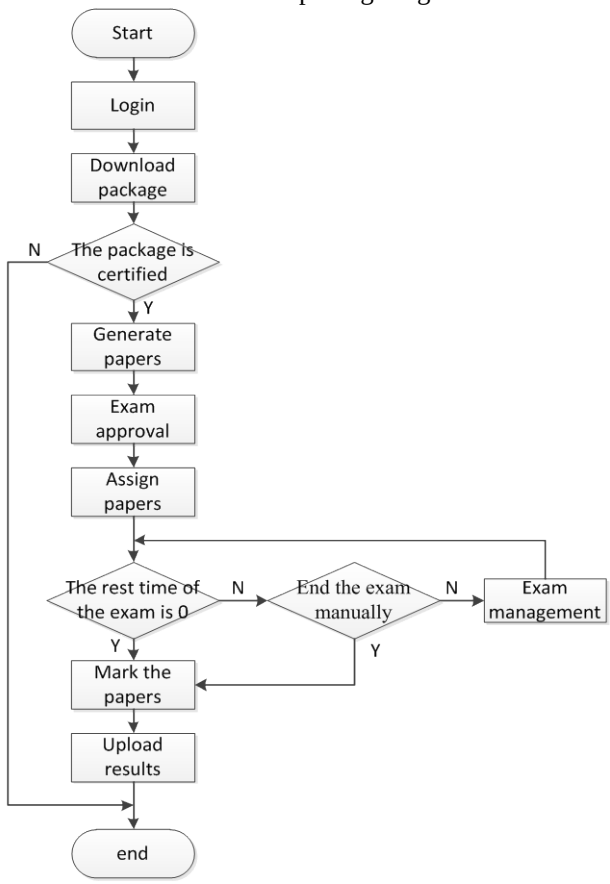


Figure 3. Examination center work flow diagram

## C. *Examination Sites*

First examination sites must initiate a connection request to the examination center. After receiving the request, the examination center will give a response and authenticate identity authentication with the examination sites. The process of identity authentication will be introduced in detail in Chapter IV. Then the examination center and examination sites have a safe communication.

The work flow of examination sites is shown in *Fig. 3*. The examination sites' manager logs on the system, downloads the exam package generated by the examination center and carries on the integrity authentication for the exam package. The authentication process will be described in Chapter IV. If the exam package is finished with fine completeness, exam paper can be generated. The exam manager approvals examination for the candidates and supervise their status and the rest time of the exam. When the exam time is over, the exam manager ends the exam

manually, and forces the student who doesn't submit papers to finish the exam. And then they correct the exam papers. Objective questions are automatically marked by computers, and subjective questions are corrected by themselves. Finally they encrypt the exam files and upload it to the examination center.

## IV. System Security Design

### *A. Identity Authentication Between Examination Center and Examination Sites*

The examination sites need to be registered if it enters the examination center for the first time. The registration process is shown in *Fig. 4*. First, examination site sends a connection request to the examination center, and after receiving the connection request the examination center gives a response for the request. Second, examination site generates a pair of key and save the private key. Third, examination site summarizes its registration information, encrypts the registration information and the message digest using the public key of the examination center and send its own public key, encrypted registration information and message digest to the examination center. Forth, when receiving the messages, the examination center decrypts them by using the private key from itself and obtains the registration information of the examination site. The message digest generated by registration information. The examination center summarizes the registration information of the test center and compares it with the message digest from the examination site to ensure that the registration information is not lost and tampered by hacker. Fifth, the examination center verifies the identity of the examination site and agrees to the site's registration application. Then the examination center randomly generates a password, use the public key sent by examination site to encrypt the password and save the public key into file. After that, the encrypted password will be sent to the examination site. Finally, examination site uses its own private key to decrypt the password and get permission to log in the center.

Examination sites need to download the candidates information and exam papers from the examination center and then can organize an examination. But prior to this, the examination center must verify the identity of the examination sites. Examination center and examination site's identity authentication process shown in *Fig. 5*. First, examination site sends a connection request to the examination center, and the center doesn't give a response until it receives the request. Second, examination site uses its own private key to encrypt the password and sends it to the examination center. Third, after receiving the password from the examination site, the examination center finds the public key of the examination site from the document, and use this public key to decrypt the password. When the legitimacy of the password is judged, the normal communication with the center is established.

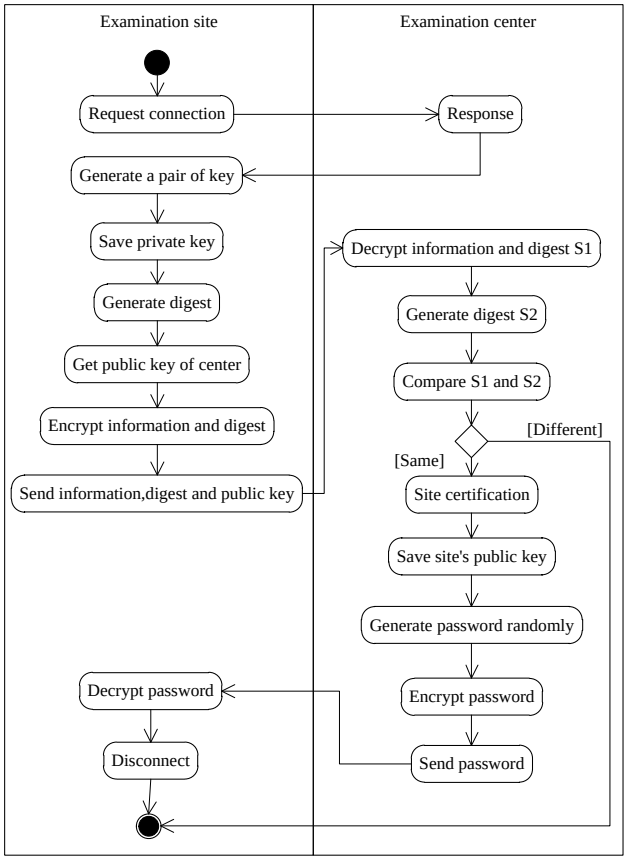


Figure 4. Examination sites registration's activity chart

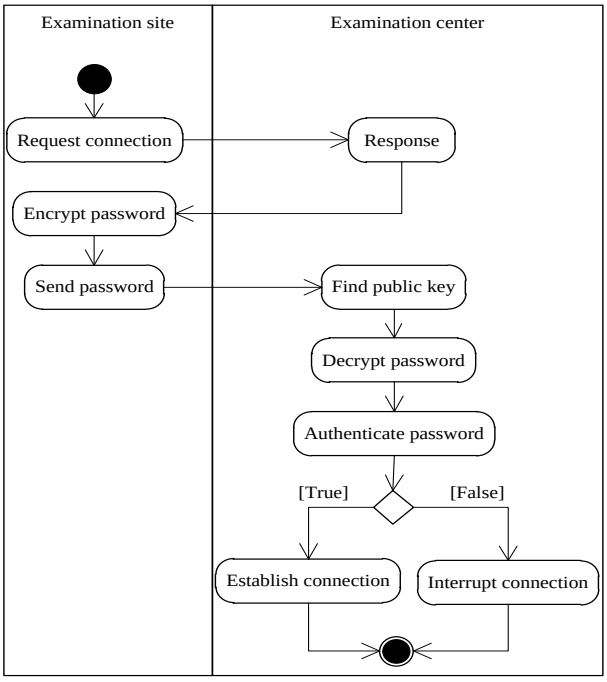


Figure 5. Identity certification between examination center and examination site

### *B. Signature and Certification of Exam Paper Package*

The exam paper package is the core of the examination process which contains the most important data for the whole examination. So it is important to ensure the confidentiality and integrity of the package. In the package transmission process, we must ensure that the data in the package not only can be stolen by illegal users, but also can prevent data loss, data tampered and other anomalies. So we need to encrypt the exam package, and certificate its integrity.

The integrity authentication of the exam package process shown in *Fig. 6*. As can be seen from Section A in this chapter, after the certifying identity, examination center and examination site can carry out normal communication.

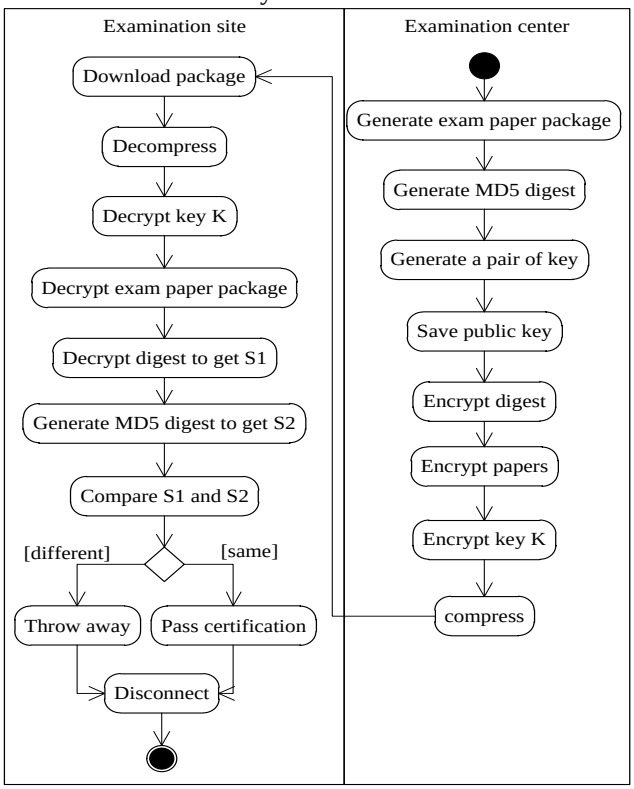


Figure 6. Exam package integrity verification activity chart integrity authentication

First of all, the examination center generates a set of papers, and the papers are summarized to message digest with MD5 algorithm. Second, the examination center produces a pair of key with RSA, encrypts the digest using the private key and stores the public key in the file. Third, the examination center uses the symmetric key algorithm to encrypt the papers. We uses DES algorithm for encryption and the symmetric encryption key is K. Forth, the examination center finds the document to obtain the public key of the examination site and encrypts the key K using this public key to obtain E(K). Finally, the examination center compresses encrypted papers, message digest and E(K) to a package.

Examination site downloads the signed package from the examination center and decompresses it. Then, The site decrypts E(K) using its own private key and obtain the symmetric key K. After that, the site uses the symmetric key K to decrypt the papers and obtain the examination information. The site obtains the public key of the center and uses it to decrypt the message digest in order that it can obtain the digest S1 sent by the examination center. Finally, the site summarizes the decrypted papers by MD5 algorithm, gets the digest S2. The site contrasts S1 and S2, if the same, it proves that the exam paper is complete, and it can pass certification. Otherwise, it cannot.

### *C. Data Encryption*

Sensitive data in the database, such as, user's password, the answer to the papers, candidates' answer, stored in the database with plain text will also become a major security risk. So the sensitive data encryption is also an indispensable link. In addition to using high-intensity RSA encryption algorithm to encrypt data in the system, you can also choose the faster XOR encryption according to the actual need of security.

If A is the information you want to encrypt, there is a key B, A and B do XOR, get C is encrypted information that can be transmitted. Get C, only by doing XOR with B can you get the original information A. If it is applied to a string, each character on the string represents a string of binary numbers. In the database, the data are stored with the String type, in order to facilitate the string operation and avoid produce illegal characters, so we use @ to separate each byte in database. You must split the string based on the @ first when we do decryption to get the character array and then decrypt the message. The decryption process is the same as the encryption process.

## V. CONCLUSION

The distributed examination system, which is designed and implemented by separating examination sites from the examination center, is based on the MVC model and implemented by the J2EE framework. The system uses a variety of security means to design and implement an examination system that can ensure the safe communication between the examination center and examination sites. This system effectively improves the concurrent access ability and breaks down the pressure of the examination center. The paper focuses on the confidentiality and integrity in the data transmission process. And it also concentrates on improve the security of the examination system by identity authentication, data encryption and data integrity authentication. This system design considers system practicality, information confidentiality, exam security, fairness, etc., It is suitable for candidates in the new era.

## REFERENCES

[1] Yuan Bing, Yang Cheng. Design of Distributed Examination System Based on Task[J]. Computing Engineering and Design, 2011, 32(10): 3530-3533.

[2] Li Gang. Lightweight Java EE enterprise applications in actual combat:Struts 2+Spring 4+Hibernate Integrated development[M]. Electronic Industry Press, 2014.

[3] Duan Zhengmin. Research and Implementation of Identity Authentication Technology[D]. Chongqing University, 2004.

[4] Teanbaumu, Weaselor. Computer Network (5th Edition)[M]. Tsinghua University Press, 2012.

[5] Cheng Fenhua. Design and Realization of Distributed Examination Sy stem[J]. Computer and Digital Engineering, 2005, 33(11):142-144.

[6] Dong Jiumin, LiuYong. Design and Realization of Distributed Test S ystem Based on .NET and COM+[J]. Electronic Design Engineering, 2010, 18(7):82-84.

[7] Wang Huaxiang. Design and Implementation of Internet Distributed Examination System[J]. Computer Engineering and Design, 2006, 27( 12):2294-2297.

[8] Li Xia. Distributed Online Examination System Design and Impleme ntation Based on the Internet[J]. Network Security Technology and A pplication, 2014(8):27-27.

[9] Liu Yuping. Application of Data Encryption in Computer Security[J]. INFORMATION & COMMUNICATION, 2012(2):160-161.