The Research and Application of Cloud Printing Platform Based on Improved AES-RSA Encryption Algorithm

Yalin MIAO, Huanhuan JIA, Xuemin LIU, Yang ZHANG, Weihao TAN
Xi'an University of Technology,
School of Printing, Packaging Engineering and Digital Media Technologys
Xi'an ,China
7673684@qq.com; 1607421431@qq.com

***Abstract*—With the development of cloud computing and Internet technology, the traditional printing mode can no longer meet the needs of users, so the cloud printing mode comes into being. However, most of today's Cloud Print operators only focus on the introduction of special services, while ignoring the security factors to ensure the operation of the platform, and there are hidden dangers of personal file information leakage. In view of the shortcomings of traditional printing methods, this paper takes the Internet as the starting point, integrates printing resources, builds a shared printing platform, and provides convenient printing services for cloud printing users. At the same time, Hash algorithm is added on the basis of AES-RSA hybrid encryption algorithm, and the algorithm is combined with software functions to effectively solve the security problems existing in the existing cloud printing platform.**

Keywords— Cloud printing ; File security ; Hybrid encryption

I. INTRODUCTION

Cloud computing and Internet technologies affect the production and business activities of all walks of life. The printing method has also evolved from the original local printing to the current "cloud printing" [1]. Cloud Printing integrates virtualized print resource network and centralizes management, which enables users to enjoy on-demand services through any terminal connected to cloud printing platform in any network area [2]. The combination of cloud manufacturing technology and printing industry has made printing resources more efficient and transformed into a new network printing mode. Nowadays, cloud printing has become the focus of research on printing mode [3].

At present, the research results of cloud printing at home and abroad have been put forward continuously [4],[5]. In April 2010, Google took the lead in putting forward the concept of cloud printing, introducing Chrome OS with cloud printing function, which integrates cloud printing server into Chrome browser and makes it easy for users to add printers to their Google accounts at will, without requiring special printer driver and control software [6]. Based on Google Cloud Printing, Hewlett-Packard used smart terminal devices to control access to printers. By assigning email addresses to printers, users could complete printing by sending files to assigned addresses at will [7]. Other manufacturers have also made relevant positive exploration and in-depth research. Apple's cloud printing technology was achieved through the combination of Apple-Air Print and EFI technology. Epson created a unique mobile printing service Epson Connect after continuous research in 2011 [8]. Some scholars have also done some research on cloud printing technology. Harish Kamath and ridhar Solur have proposed a cloud printing technology scheme that registers printers in cloud printing servers and sends printing requests to them using portable electronic devices to complete printing operations [9]. Rajesh Bhatia proposed a hybrid cloud printing service system with flexibility of public cloud printing service and security of private cloud printing service [10]. However, cloud printing services also have drawbacks. Alex Wawro pointed out that although the cloud printing technology proposed by Google and HP can realize users' printing needs by connecting to the Internet from any mobile device anywhere, it is because of these that cloud printing service has certain security risks[11].

As an advanced technology,cloud printing is bound to become the trend of the future market. However, there are still many shortcomings in cloud printing technology, the most prominent of which is the security risk [12]. In view of the shortcomings of traditional printing methods, this paper takes the Internet as the starting point, cloud printing as the center, integrates printing resources, and builds a shared printing platform. It can realize personal information service, document printing, document encryption and decryption, help and service, resource sharing and nearby search, and provide convenient printing service for cloud printing users. At the same time, Hash algorithm is added on the basis of AES-RSA hybrid encryption algorithm, and the algorithm is combined with software functions to effectively solve the security problems existing in the existing cloud printing platform.

II. ENCRYPTION ALGORITHM

A. AES Symmetric Encryption Algorithm

Symmetric encryption algorithm refers to encryption and
decryption using the same key, or between the two can be derived from each other. AES symmetric encryption algorithm processes the input data in groups. When encrypting and decrypting, the input data is divided into 128 bits, which is represented by a 4*4 state matrix. Similarly, the secret key is represented as a state matrix. In a matrix, bytes are sorted by columns, and all subsequent transformations are based on matrices [13]. After N rounds of iteration, the result is still a 4*4 state matrix, which is restored to ciphertext. The first N-1 round consists of four

different transformations: SubByte, ShiftRow, MixColumn and AddRoundKey [14]. The last round does not contain column hybrid transformation. In front of the first round, there is a reserve wheel, which only contains AddRoundKey.

B. RSA Asymmetric Encryption Algorithm

RSA algorithm is a block cipher system, which needs to digitize the plaintext before grouping, and then carry out block encryption [15]. In the encryption process, if user *a* wants to encrypt plaintext *m* and sends it to user *b*, user *a* finds the public key $\{e,n\}$ of user *b* in the database. Grouping plaintext M into $M=m_1m_2\cdots m_r$. Make an encryption change for each group, that is, $c_i=m_i^e(\mathrm{mod}\,n)$ for $i=1,\cdots r$, and pass ciphertext $C=c_1c_2\cdots c_r$ to user *b*. In the decryption process, after receiving the ciphertext $C=c_1c_2\cdots c_r$, the user *b* first performs a $m_i=c_i^d(\mathrm{mod}\,n)$ decryption operation on each $c_i(i=1,\cdots,r)$, and then merges the packets to obtain $M=m_1m_2\cdots m_r$, which is the plaintext transmitted by the user *a*.

C. Hash one-way hash function

The Hash one-way hash function in digital signature technology can guarantee the integrity of information content during file transmission. The Hash function inputs a variable-length data block to produce a fixed-length Hash value of $h=H(M)$ [16]. There are many common one-way hashing algorithms. The most widely used hash function is SHA-1. The SHA-1 function is very efficient both in terms of security and computational efficiency. In order to verify the integrity of the data, this paper selects the SHA-1 function to encrypt the file and the symmetric key in the AES encryption algorithm. The SHA-1 algorithm groups the plaintext. Each group is 512 bits long. The length is insufficient to fill 512 bits according to certain rules. The 512-bit group is divided into 16 32-bit subgroups, which can be recorded as: $h=H(M)$. After a certain rule transformation, five 32-bit information variables are calculated, and the five variables are combined to become a 160-bit information digest.

D. Improved AES-RSA Encryption Algorithm

This paper combines AES symmetric encryption algorithm with RSA asymmetric encryption algorithm, which not only takes advantage of the high computational efficiency of symmetric encryption algorithm, but also takes advantage of the high security of asymmetric encryption algorithm. The sender knows the receiver's public key beforehand before sending the information. First, it uses symmetric encryption algorithm to encrypt the information. Then it uses public key asymmetrically to encrypt the symmetric key and sends the ciphertext to the receiver together with the encrypted symmetric key. After receiving the information, the receiver decrypts the symmetric key with his private key and decrypts the ciphertext with the decrypted symmetric key, thus obtaining the plaintext information. However, this encryption algorithm fully trusts the encryption and decryption process, and does not verify whether the plaintext information before and after encryption and decryption is consistent.

Hash algorithm has the characteristics of unidirectionality and anti-collision. It can verify the integrity of files, which makes up for the shortcoming that hybrid encryption algorithm does not verify the integrity of files. At the same time, cloud printing platform will inevitably involve some files with large amount of data. If the symmetric key of the file is destroyed during transmission, the receiver can only get a bunch of random codes after receiving the file and decrypting it. This is not the result we want, and it takes some unnecessary time. In this paper, Hash algorithm is also used to extract abstracts of symmetric keys. When decrypting, the consistency of symmetric keys before and after encryption and decryption is verified. If the subsequent decryption process is not consistent, the server load will be reduced. The encryption and decryption process of the improved AES-RSA encryption algorithm is shown in Figure 1.

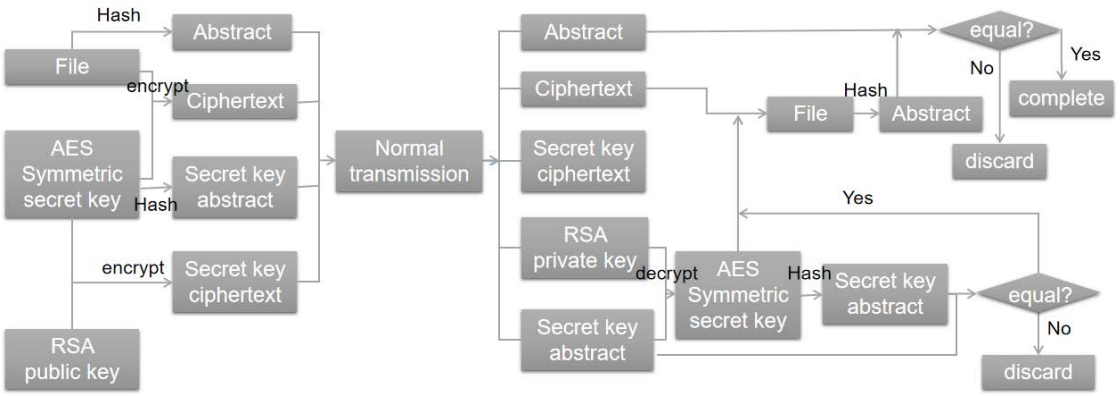

Figure 1 Improved AES-RSA encryption algorithm

The specific encryption process is as follows:

1)Using AES symmetric encryption algorithm to encrypt files.

2)The public key in RSA asymmetric encryption algorithm is used to encrypt the symmetric key in AES symmetric encryption algorithm to make up for the

protection and management of the key in AES encryption algorithm.

3) To verify the consistency of symmetric keys and files before and after encryption and decryption, SHA-1 security hashing algorithm is used to extract abstracts of file and symmetric keys in AES symmetric encryption algorithm.

4)The plaintext digest, ciphertext, key digest and symmetric key ciphertext are transmitted together.

The specific decryption process is as follows:

1) Using RSA private key to decrypt AES key ciphertext and extracting the digest of decrypted AES key.

2) Comparing the digest of the decrypted AES key with the digest of the transmitted key. If they are inconsistent, it means that the data has been lost or destroyed, then it needs to be resent, and if they are consistent, the next step will be taken.

3) The decrypted AES symmetric key is used to decrypt the ciphertext and extract the abstract at the same time.

4) Comparing the digest of the decrypted file with the digest of the directly transmitted file. If the two are inconsistent, the data in the file has been lost or destroyed, and if the two are consistent, the consistency of the file will be verified.

III. System Architecture Design

To ensure the extensibility, maintainability and security of the system, the cloud printing service management platform developed in this paper adopts a distributed architecture based on B/S network architecture. According to the users'needs of cloud printing service platform, we divide function modules, analyze business processes, and determine that the platform is finally constructed by distributed architecture, including infrastructure layer, basic data layer, technology platform layer and application platform layer. The physical foundation of the platform is constructed by infrastructure layer, and the basic data layer is used to manage platform-related data and technology platform layer. Provide the development environment and technology of the whole platform. The application platform layer realizes all the functions of the platform, as shown in Fig. 2.

Infrastructure layer: mainly hardware equipment, including network and communication facilities and printing equipment, provides basic operation guarantee for data transmission and document printing of the platform.

Basic Data Layer: During the operation of the whole platform, users will generate relevant data, including user information, file order information and order status information, and the relationship between these data, such as the relationship between customers and file orders, the relationship between service providers and file orders, and the relationship between orders and order status.

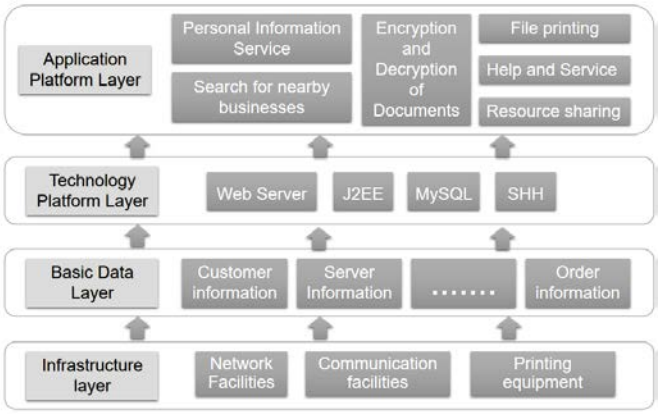

Figure 2 Overall framework diagram of the platform

Technical Platform Layer: Provide development support and technical support for the whole platform, mainly including the B/S architecture, Java + Apache + MySQL mode, SSH software development framework technology and so on.

Application Platform Layer: It mainly includes two parts: one is the customer application system, which realizes the interaction with customers. The other is the business management system, which serves the managers of service providers. It realizes the functions of personal information service, document printing, document encryption and decryption, help and service, resource sharing and nearby business search. It realizes the function of human-computer interaction through friendly window interface, and provides users with visual application services.

IV. Technical Architecture Design

This paper adopts SSH software development framework technology which combines Struts 2, Spring and Hibernate. The principle of integrating SSH framework is shown in Figure 3.

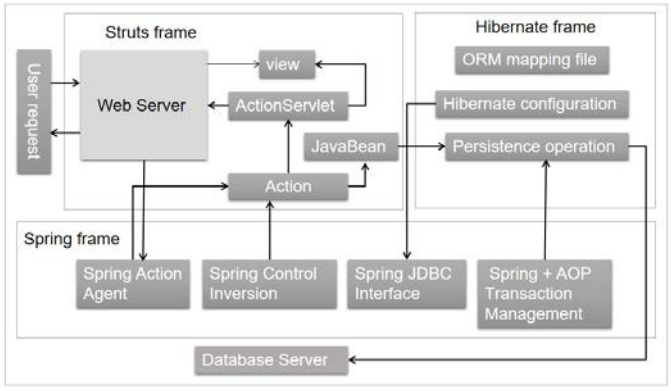

Fig. 3. Principle of the SSH frame

Struts 2 is the basis of the whole framework, mainly responsible for the separation of MVC and business jump. Hibernate framework provides support for the persistence layer to achieve the correct conversion between instance objects and relational databases.Spring manages Struts 2 and Hibernate. The division of labor among layers is detailed, the decoupling between layers is realized, and the code is more flexible.

V. Algorithmic Performance Analysis of Platform

According to the business process of the platform, the whole printing task can be divided into two processes: uploading and downloading. In the process of uploading, files are read in the form of encryption stream, while in the process of downloading, files are written in the form of decryption stream. In this paper, the decryption process is equivalent to the inverse operation of the encryption process, which is explained here only by the encryption process.

For the comparison of encryption strength, the encryption strength of the improved AES-RSA encryption algorithm used in this platform is much higher than that of AES encryption algorithm and RSA encryption algorithm. In this paper, AES symmetric encryption algorithm and RSA asymmetric encryption algorithm are respectively compared with the improved AES-RSA encryption algorithm used in this platform for encryption efficiency and encryption time, and the experimental results are analyzed. The encryption rate and encryption time comparison between AES algorithm and the improved AES-RSA algorithm is shown in Tab.1 and Fig. 4.

TABLE I Encryption rate of AES and improved AES-RSA

File Size (M)	AES Algorithm (M/S)	Improve AES-RSA (M/S)
1.06	6.15	6.09
3.15	7.83	7.76
5.49	8.13	8.06
7.12	7.52	7.46
9.23	7.75	7.69
22.0	8.05	8.01
55.3	7.99	7.98
77.8	8.16	8.15
Average Value	7.69	7.65

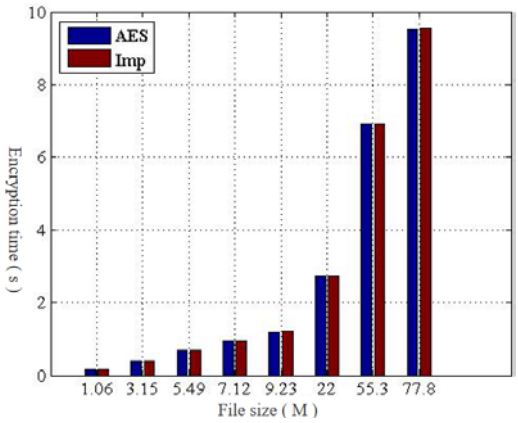

Fig. 4. Encryption time of AES and improved AES-RSA

Tab.1 and Fig. 4 show that compared with the single AES encryption algorithm, the improved AES-RSA encryption algorithm used in this platform has almost the same encryption efficiency and encryption time, and the difference for files of about 10M is only milliseconds. It is completely within the user's acceptance range and does not affect the user experience of cloud printing service platform. The encryption rate and encryption time comparison between RSA algorithm and the improved AES-RSA algorithm is shown in Tab.2 and Fig. 5.

TABLE II Encryption rate of RSA and improved AES-RSA

File Size （K）	RSA Algorithm （K/S）	Improve AES-RSA （K/S）
79	35.70	3038
236	38.36	4538
393	38.38	4570
550	38.50	4583
707	38.54	5086
864	38.48	5333
1021	38.35	5519
1178	38.27	5636
Average Value	38.07	4788

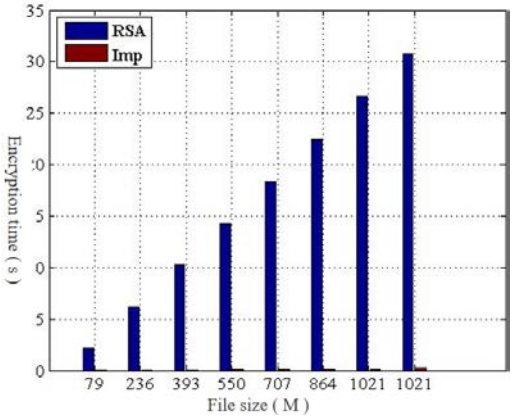

Fig. 5. Encryption time of RSA and improved AES-RSA

Tab.2 and Fig. 5 show that the improved AES-RSA encryption algorithm used in this platform is much more efficient than the single RSA encryption algorithm, and the encryption time is much lower than the RSA encryption algorithm, so it has high practicability.

VI. Summary

In this paper, cloud printing service platform based on hybrid encryption algorithm is studied, the shortcomings of current cloud printing platform are analyzed, and a new cloud printing service management platform based on improved AES-RSA encryption algorithm encryption algorithm is designed. Hash algorithm is added on the basis of AES-RSA hybrid encryption algorithm, which combines the algorithm with software functions, and effectively solves the security hidden dangers existing in the existing cloud printing services. A secure and shared printing platform is constructed to improve the office efficiency of individuals and enterprises and provide users with convenient and reliable printing services.

VII. Acknowledgment

This work was supported by the 2017 Xi'an Science and Technology Project, number: 2017050NC/NY011(1).We thank senior engineer Yilong Xiao for excellent technical support and value able discussion.

REFERENCES

[1] Wang Siwu. Problems and Countermeasures of cloud printing service [J]. Statistics and management, 2014 (9): 41-43.

[2] Zhang Neng. Research on Cloud Printing Service and Scheduling Technology [D]. Guilin University of Electronic Science and Technology, 2015.

[3] Zeng J, Jackson S, Lin I J, et al. Operations simulation of on-demand digital print [C]// Conference Anthology, IEEE, 2014:1-5.

[4] Zhu Y, Wu W, Wu L, et al. Smart Print: A Cloud Print System for Office [C]// IEEE Ninth International Conference on Mobile Ad-Hoc and Sensor Networks. IEEE, 2013:95-100.

[5] Leeladevi B, Raj C P R, Tolety S. A study on smartphone printing approaches [C]// Information & Communication Technologies. IEEE, 2013:707-711.

[6] Li Chunquan, Mo Huiguang, Shang Yuling, et al. Research on equipment access technology in cloud printing environment [J]. Modular machine tools and automatic processing technology, 2017 (6): 78-81.

[7] Muzi.Cloud Printing'makes our life more wonderful [J]. Network and Information, 2011, 25 (11): 41-41.

[8] Zheng Xilong, Yang Yong. Road from Cloud Printing to Cloud Printing [J]. Printing Today, 2014 (11): 36-38.

[9] Kamath H, Solur S, Pitkin D, et al. Cloud printer with common user print experience: US, WO 2011090474 A1[P]. 2011.

[10] Bhatia R. Printer identification validation procedure on a cloud computer system to recognize the target printer: US, US8976388[P]. 2015.

[11] Wawro A. Cloud Printers Rain on Security Parade[J]. Pcworld, 2011,29(4):36.

[12] Wang Na, Lu Zhiyong. An application example of cloud printing based on private network [J]. China New Communications, 2012 (21): 63-64.

[13] Oukili S, Bri S. High speed efficient advanced encryption standard implementation[C] // International Symposium on Networks, Computers and Communications. IEEE, 2017:1-4.

[14] Mo Jianhua. An encryption algorithm for WSN data security [D]. Zhejiang University of Technology, 2010.

[15] Research on Sun Jing. RSA Encryption Algorithms [J]. Modern Economic Information: Academic Edition, 2008 (5).

[16] Liu Qi. Design and implementation of online password cracking system [D]. Dalian University of Technology, 2015.