Study of Encrypted Transmission of Private Data During Network Communication: Performance Comparison of Advanced Encryption Standard and Data Encryption Standard Algorithms

Dongliang Bian, Jun Pan and Yanhui Wang*

Department of Computer Information Engineering, Baoding Vocational and Technical College, Baoding 071000, Hebei, China
E-mail: byhv30@163.com
**Corresponding Author*

Received 09 August 2022; Accepted 31 October 2022;
Publication 03 December 2022

Abstract

The involvement of the Internet in the production of daily life has increased the demand for the security of private data on the Internet. This paper briefly introduced the principles of advanced encryption standard (AES) and data encryption standard (DES) algorithms and then conducted simulation experiments on the two encryption algorithms in a laboratory server. The results showed that both algorithms had excellent sensitivity to plaintext keys, and the sensitivity of the AES algorithm was higher; the encryption and decryption time of both algorithms increased as the file got larger, and the encryption and decryption time of the same algorithm was not much different; the encryption and decryption time of the AES algorithm was less than that of the DES algorithm for the same file, and the time taken to crack the AES-encrypted data by brute force was also much longer; during

Journal of Cyber Security and Mobility, Vol. 11_5, 713–726.
doi: 10.13052/jcsm2245-1439.1154

the transmission of encrypted data, as the data increased, the integrity of the ciphertext decryption by the third-party decreased, and the integrity of the AES algorithm-encrypted file was significantly smaller than that of the DES algorithm-encrypted file when it was decrypted.

Keywords: Network data, encryption, data encryption standard, advanced encryption standard.

1 Introduction

With the involvement of the Internet in daily life, people's life has become more and more convenient, such as the easier and faster information communication and the online cashless shopping [1]. However, in the process of receiving convenient services from the Internet, users are often required to provide information that proves their identity to ensure the accuracy of Internet services, and such information is usually important private information. Although the operators providing Internet services promise not to disclose users' private information [2], there is a possibility that such information will be intercepted and stolen in the transmission process. Once the leaked private information is used by unlawful elements, it will have adverse effects on both users and regular operators, so the security of private information transmission needs to be improved. Encrypting transmitted data is a common way to improve data transmission security [3]. In order to ensure the security of users' private data during transmission, on the one hand, a more secure transmission method can be chosen from the physical layer, such as wired transmission or improved wireless channels; on the other hand, the transmission content can be encrypted to protect the private information even if it is stolen by criminals [4]. Usually, these two methods are applied together, but this paper focuses on the encryption algorithm of data. Guo et al. [5] proposed an image encryption scheme based on fractional-order chaotic time series. The experimental results showed that the key space was large enough to resist brute force attacks and the encrypted image had a random distribution of gray values. Yoon et al. [6] proposed a density-based data encryption scheme and a database outsourcing query processing algorithm. The performance analysis found that the scheme had better query processing performance than the existing schemes, ensuring the user's privacy. Xue et al. [7] proposed an improved, efficient data encryption method, which was based on ciphertext policy attribute encryption and used fixed-length ciphertext to control the

time overhead. The simulation experiments showed that the improved algorithm had high reliability. This paper briefly introduced the principles of two encryption algorithms, data encryption standard (DES) and advanced encryption standard (AES), and performed simulation experiments on the two encryption algorithms in a server in the laboratory.

2 Network Data Encryption Algorithm

The algorithms used to encrypt data for network transmission are divided into symmetric encryption, asymmetric encryption, and hash encryption. Among them, hash encryption uses a hash function to encrypt plaintext data [8]; however, the hash function encrypts plaintexts of different lengths to obtain ciphertexts of the same length, which will lose some information, and the relatively complicated encryption process is difficult to cope with the increasing network data [9]. Asymmetric encryption uses a key pair to encrypt and decrypt the plaintext, where the key pair is divided into a public key and a private key. The public key encrypts the plaintext, and the private key held by the individual user decrypts the ciphertext. Although the encryption process of asymmetric encryption also has some complexity, compared with hash encryption, the ciphertext obtained by asymmetric encryption will not be fixed to the same length, and the information contained in it will not be compressed [10]. Symmetric encryption uses the same key for both encryption and decryption. If the key is compared to a road, the encryption process is equivalent to walking forward along the road, while the decryption is walking back along the road. In the process of encryption and decryption, a symmetric encryption algorithm is simpler and more suitable for processing large data on the network. However, the drawback is that when using a single key for encryption or decryption [11]. Once the key is cracked or stolen, then the information within the ciphertext is exposed, and the third party who has the key can modify the ciphertext after intercepting it and then send it to the receiver [12].

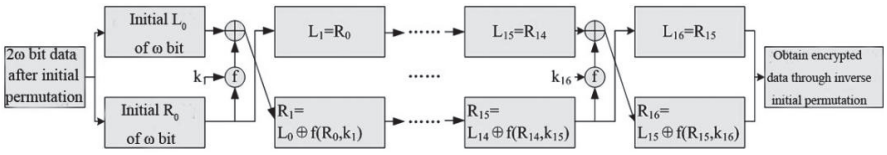


Figure 1 The basic flow of the DES algorithm.

2.1 DES Algorithm

The DES algorithm is a symmetric encryption algorithm in which the key used in the encryption process can also be used to decrypt the corresponding ciphertext. Since the same key is used for encryption and decryption, the encryption efficiency is high. Figure 1 shows the basic flow of the DES algorithm. Since the DES algorithm can only encrypt 64-bit data [13], when encrypting plaintexts with characters longer than 64 bits, the plaintexts need to be grouped according to the 64-bit specification first, and then every group is encrypted according to the flow in Figure 1.

(1) The plaintext is divided into two strings, the initial left string L_0 and the initial right string R_0, after the initial permutation (IP).

(2) Sixteen rounds of alternate encryption are performed on the left and right strings with the following encryption formula:

$$\begin{cases} L_n = R_{n-1} \\ R_n = L_{n-1} \oplus f(R_{n-1}, k_n) \\ n = 1, 2, 3, \ldots, 16 \end{cases} \tag{1}$$

where n is the number of encryption rounds, up to 16, L_n and R_n are the left and right strings after the first round, k_n is the key used for the n-th round of encryption, which is extended from the master key k, and $f(R_{n-1}, k_n)$ is the f transformation of DES encryption that takes R_{n-1} and key k_n as input.

(3) After 16 rounds of alternate encryption, L_{16} and R_{16} are merged, followed by the inverse IP to obtain the encrypted data finally.

In the above encryption process, the f transformation with R_{n-1} and key k_n as input is the core of the DES algorithm. In f transformation, the E box is used to expand the 32-bit R_{n-1} to 48-bit data, the exclusive or operation is performed on key k_n and 48-bit R_{n-1}, the table-lookup operation is performed on the computation result using the fixed table of S box [14] to convert the 48-bit data back to 32-bit, and the shift operation is performed on the 32-bit data using P box.

2.2 AES Algorithm

The AES algorithm [15] is also a symmetric encryption algorithm. It can encrypt plaintext with a length of 128 bits, so for the plaintext that is longer than 128 bits, it needs to be grouped, 128 bits in each group. If the bit length

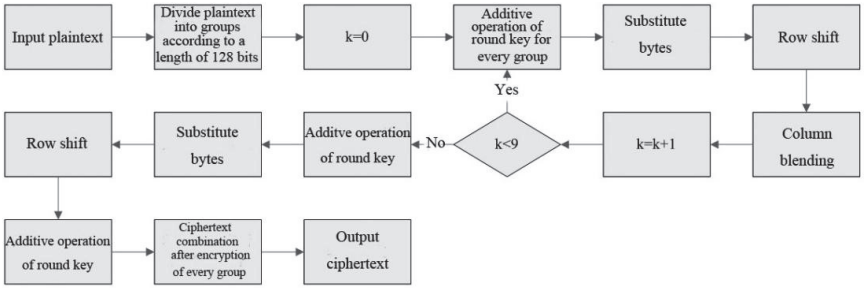


Figure 2 The encryption process of the AES algorithm.

is less than 128 bits in a group, the remaining bits are complemented by 0. The AES algorithm can encrypt every group of plaintext to 128-bit, 192-bit, and 256-bit. In this paper, a 128-bit key is used for encryption, and Figure 2 shows the basic flow of encryption.

(1) The plaintext to be encrypted is input [16] and grouped according to the length of 128 bits. The group that is less than 128 bits is supplemented with 0. A byte consists of 8 bits, so 128-bit plaintext has 16 bytes. Then, the bytes are arranged in a 4×4 matrix from top to bottom and from left to right in order. Moreover, $k = 0$.

(2) Every group is encrypted using the round key, i.e., an additive operation is performed on the bytes to be encrypted and the round key. The round key also has 128 bits, i.e., 16 bytes, and the 16 bytes form a 4×4 matrix [17].

(3) The encrypted bytes are replaced using the S box of the fixed table of the AES algorithm. The S box is a 16×16 table in the AES algorithm, and the elements in the table are the byte elements used for replacement. When the bytes are replaced by the S box, the first four bytes are used as the rows of the S box, and the last 4 bytes are used as the columns of the S box. The original bytes are replaced by the S-box elements corresponding to the column and row.

(4) Row shift is performed on the 4×4 matrix that has been treated by byte replacement. The specific operation is to cyclically shift elements in every row in the matrix according to the preset displacement [18].

(5) The column blending operation is performed on the matrix after row shifting: multiplying the matrix by a given 4×4 matrix used for column blending. Then, $k = k + 1$.

(6) Whether k is less than 9 is determined. If yes, it returns to step (2); if not, the round key encryption, byte substitution, row shift, and round key encryption are performed on the matrix in turn.

(7) The AES-encrypted ciphertext is obtained by combining groups of ciphertexts processed by the above steps.

3 Simulation Experiments

3.1 Experimental Environment

The experiment was carried out on a server in the lab. Three sets of servers were needed for the simulation experiments, one for encrypting the data, one for decrypting the data as a receiver, and one as a third party to simulate a hacker intercepting the data. The servers had 16 G memory, a Core I7 processor, and a 64-bit Windows operating system.

3.2 Experimental Project

(1) Plaintext and key sensitivity test of the algorithm

When the algorithms were tested for plaintext sensitivity, two number plaintexts, "1234567890" and "1234567899", and two letter plaintexts, "abcdefghij" and "abcdefghii", were given. There was only one character difference between the two plaintexts, and the key of both encryption algorithms was set as "32568894". After encryption by the two algorithms, the results of the number and letter plaintexts were recorded.

When the key sensitivity of the algorithms was tested, plaintexts "1234567890" and "abcdefghij" were given, and then two keys, "32568894" and "32568899", were set. The difference between the keys was only one character. The encryption results of the two algorithms after applying the keys were recorded.

(2) Encryption efficiency test of the algorithm

The encryption efficiency of the two algorithms was tested using three formats of files, including images in the jpg format, audios in the mp3 format, and documents in the text format. The set of every document format included 1 MB, 10 MB, and 100 MB documents, ten for each size.

When the algorithm encryption efficiency was tested, both algorithms used key "12354678" to encrypt the document sets of the three formats. The average encryption time for every file size in different formats was recorded.

(3) Security test of the algorithm

The DES-encrypted and AES-encrypted files obtained from the encryption efficiency test project in the previous section were used to test the security of the two encryption algorithms. The legal decryption time of encrypted images, audios, and documents in sizes of 1 MB, 10 MB, and 100 MB under both DES and AES encryption algorithms were examined first. Then, the average time consumed by the algorithm to legally encrypt 1 kb, i.e., the average time taken to decrypt 1 kb ciphertext using a single key in the encryption algorithm, was calculated.

Then, the time taken to crack 1 kb ciphertext with brute force was calculated based on the time taken to decrypt 1 kb ciphertext by a single key. Since the brute-force cracking of a ciphertext was performed by traversing all possible keys, the time taken to encrypt a 1kb ciphertext with a single key in the encryption algorithm was multiplied by the number of keys that could be employed in the algorithm to obtain the time taken to crack 1 kb ciphertext with brute force under this encryption algorithm.

(4) Attack resistance test of the algorithm

Packets in a size of 5 MB, 15 MB, 25 MB, 35 MB, and 45 MB were prepared, 100 each size. The packets were encrypted and transmitted from server 1 to server 2 via server 3. Then, server 3 decrypted the encrypted packets to simulate the situation that the encrypted data were attacked by the third party during the network communication. The time limit for a third-party server to crack the encrypted data was 60 min, and the cracked ciphertext was compared with the original text to obtain the decryption integrity [19]. The attack resistance of DES and AES algorithms was compared.

3.3 Experimental Results

This paper first tested the plaintext and key sensitivity of DES and AES algorithms, and Table 1 shows the test results. In the plaintext sensitivity test results, even with the same plaintext and key, the encryption results of the two encryption algorithms were completely different; with the same key, the ciphertext obtained by the two encryption algorithms changed after a one-character change in the plaintext, among which the change in the ciphertext encrypted by the AES algorithm was the most, and the change in the ciphertext encrypted by the DES algorithm was concentrated in the second half; with the same plaintext, the ciphertext of the two encryption algorithms changed after a one-character change in the key, and the changes were similar.

Table 1 Plaintext and key sensitivity test results of two encryption algorithms

Plaintext sensitivity test	Plaintext	1234567890	1234567899	abcdefghij	abcdefghii
	Key	32568894			
	Encryption results of the DES algorithm	87NHUYT568RFDE	87NHUYT567FGTRQ	684FHTJU8524FD	684FHTJU85GTUB
	Encryption results of the AES algorithm	568DGHJOHI54QD	524RFTYHY546GH77	GH4656874GHTQ	74GHTQGH465UI
Key sensitivity test	Plaintext	1234567890		abcdefghij	
	Key	32568894	32568899	32568894	32568899
	Encryption results of the DES algorithm	87NHUYT568RFDE	7856TGFRW568RF	GHJ565RTE638GH	KMNJHG564GTRA
	Encryption results of the AES algorithm	568DGHJOHI54QD	32479RHYDU674H	NHGJ84FR9YD56Y	NHGGHJ565NJHG

Table 2 Time taken by the two encryption algorithms to encrypt files in three formats and three sizes

File Format	Encryption Algorithms	Encryption Time for 1 MB/s	Encryption Time for 10 MB/s	Encryption Time for 100 MB/s
Image (jpg)	DES	6.854	71.245	612.323
	AES	3.687	40.213	399.325
Audio (mp3)	DES	6.547	68.756	621.235
	AES	3.558	39.864	401.236
Document (txt)	DES	6.456	69.368	6322.413
	AES	3.546	39.457	410.328

In the simulation experiment, three file formats, namely, image, audio, and document, were also tested, and the encryption time of the two algorithms for files of different sizes was recorded. The final results are shown in Table 2. It was seen from Table 2 that the time consumption of both encryption algorithms increased with the increase of file size regardless of the file format, and the encryption time of the DES algorithm was longer than that of the AES algorithm for the file of the same size regardless of the file format. The first reason for these results is that the number of encryption rounds of the DES algorithm was more. The second reason is that the encryption length of the AES algorithm was larger than that of the DES algorithm (128 bits vs. 64 bits), so the groups encrypted by the AES algorithm were less than the DES algorithm.

Table 3 Efficiency and brute force cracking time for decrypting files in three formats and three sizes by two encryption algorithms

Encryption Algorithms	File Format	Decryption Time for 1 MB/s	Decryption Time for 10 MB/s	Decryption Time for 100 MB/s	Average Encryption Time for 1 kb/s	Average Time Taken to Crack with Brute Force
DES	Image (jpg)	6.754	71.325	612.323	0.006291	1.437465×107 years
	Audio (mp3)	6.347	68.678	621.235		
	Document (txt)	6.256	69.452	632.555		
AES	Image (jpg)	3.867	40.236	399.458	0.004028	2.173344×1028 years
	Audio (mp3)	3.356	39.785	401.365		
	Document (txt)	3.258	39.654	410.457		

The files were decrypted, and their decryption time was recorded. The average time consumed for decrypting a 1 kb file and the average time consumed for brute-force cracking a 1 kb file were calculated, and the results are shown in Table 3. It was seen from Table 3 that the decryption time of the two algorithms increased as the size of the encrypted file increased, and the difference between the encryption time and decryption time of the same file was not large, which was because both DES and AES algorithms were symmetric encryption algorithms whose encryption and decryption processes were inverse. After calculation, it was found that the average decryption time of the DES algorithm for 1 kb file was 0.006291 s, and the average decryption time of the AES algorithm for 1 kb file was 0.004028 s. It was found that the decryption speed of the AES algorithm was faster, and the reason for this result was the same as the reason for the higher encryption speed mentioned before. The essence of brute force cracking is to decrypt the files by enumerating the keys, i.e., to decrypt with every key. The key length in the DES algorithm was 64 bits, of which 56 bits were the valid keys, so there were 2^{56} keys. The key length in the AES algorithm was 128 bits, so there were 2^{128} keys. Considering the number of keys and the average time consumed by the two algorithms to decrypt 1 kb file, the brute force cracking time consumed by the two encryption algorithms was calculated. The data in Table 3 demonstrated that the time consumed to crack the file encrypted by the AES algorithm with brute force was much longer than that by the DES algorithm.

Figure 3 shows the decryption integrity after a third party cracked the encrypted data with brute force for 60 min in the transmission process. It was seen from Figure 3 that the decryption integrity of the data encrypted by both encryption algorithms after brute force cracking decreased with the increase of the transmitted data. The reason for this result is that the data volume

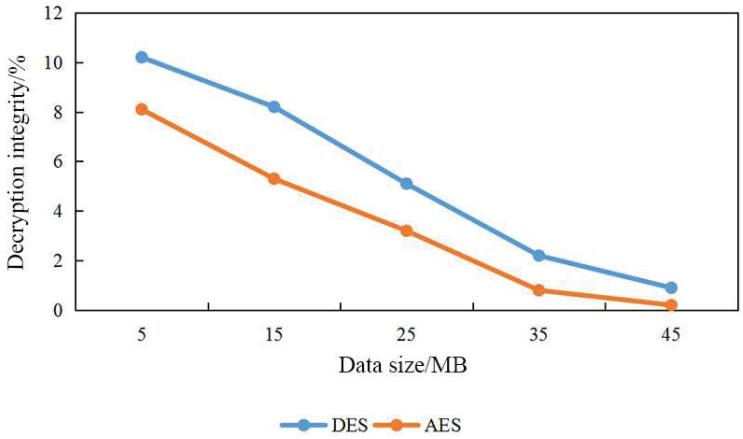


Figure 3 Resistance of the two algorithms to third-party attacks.

increased, leading to increased computation. Under the data of the same size, the integrity of the DES-encrypted files after brute force cracking was greater. The reason for this result is that the longer key of the AES algorithm not only enabled the algorithm to encrypt longer files at one time but also greatly increased the possibility of a key, which improved the difficulty of brute force cracking.

4 Conclusion

This paper briefly introduced the principles of DES and AES algorithms and conducted simulation experiments on the two encryption algorithms in the laboratory server. The plaintext sensitivity, encryption efficiency, encryption safety, and resistance to the third-party attack of the two encryption algorithms were tested. The results are as follows. Both algorithms had high sensitivity to plaintext keys, and the AES algorithm was more sensitive. When the file size became larger, the encryption time of both algorithms increased, and the encryption time of the AES algorithm was less for the file of the same size. When the size of the encrypted file increased, the decryption time of both encryption algorithms increased, but the decryption time of the AES algorithm was less for files of the same size, and the encryption and decryption time of the same algorithm was not much different. The average decryption time of DES and AES algorithms for 1 kb was 0.006291 s and 0.004028 s, respectively, and the brute-force decryption time of the AES-encrypted file was much longer than that of the DES-encrypted file.

During the transmission of the encrypted data, the data integrity of data cracked by the third-party brute force decreased as the data size increased, and the data integrity of the AES-encrypted file was lower than that of the DES-encrypted file for the file of the same size.

References

[1] Sawle P, and Baraskar T. Survey on Data Classification and Data Encryption Techniques Used in Cloud Computing. *International Journal of Computer Applications*, 135(12):35–40, 2016.

[2] Kiran G M, and Nalini N. Enhanced security-aware technique and ontology data access control in cloud computing. *International Journal of Communication Systems*, 2020(23):e4554, 2020.

[3] Teng L, Li H, Yin S, and Sun Y. A Modified Advanced Encryption Standard for Data Security. *International Journal of Network Security*, 22(1):112–117, 2020.

[4] Mihret Z, and Ahmad M W. The Reverse Engineering of Reverse Encryption Algorithm and a Systematic Comparison to DES. *Procedia Computer Science*, 85:558–570, 2016.

[5] Guo Z, Yang J, and Zhao Y. Double image multi-encryption algorithm based on fractional chaotic time series. *Open Mathematics*, 13(1):868–876, 2015.

[6] Yoon M, Jang M, Shin Y S, and Chang J W. A Bitmap based Data Encryption Scheme in Cloud Computing. *International Journal of Software Engineering & Its Applications*, 9(5):345–360, 2015.

[7] Xue S, and Ren C. Security Protection of System Sharing Data with Improved CP-ABE Encryption Algorithm under Cloud Computing Environment. *Automatic Control and Computer Sciences*, 53(4):342–350, 2019.

[8] Koukou Y M, Othman S H, and Nkiama M. Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm. *IOSR Journal of Engineering*, 06(6):01–07, 2016.

[9] Lan Z L, Zhu L, Li Y C, and Liu J. A Color Image Encryption Algorithm Based on Improved DES. *Applied Mechanics & Materials*, 743:379–384, 2015.

[10] Akbal E, Barua P D, Dogan S, Tuncer T, and Acharya UR. DesPatNet25: Data encryption standard cipher model for accurate automated construction site monitoring with sound signals. *Expert Systems with Application*, 193:1–10, 2022.

[11] Jayaprakash J S, Balasubramanian K, Sulaiman R, Hasan M K, Parameshachari B D, and Iwendi C. Cloud Data Encryption and Authentication Based on Enhanced Merkle Hash Tree Method. *Computer, Materials and Continuum (English)*, (7):519–534, 2022.

[12] Nasution A B, Efendi S, and Suwilo S. Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB). *Journal of Physics Conference*, 1007:012010–, 2018.

[13] Eltayeb G. Combination of the "Data Encryption Standard" algorithm (DES) and the 'Pub-lickey encryption' algorithm (RSA) on the keygeneration stage. *International Journal of Emerging Trends & Technology in Computer Science*, 4(4):1–3, 2015.

[14] Banushri A, and Karthika R A. A Survey on Data Security Using File Hierarchy Attribute-Based Encryption in Cloud Computing Environment. *Journal of Advanced Research in Dynamical & Control Systems*, 2017(4):144–149, 2017.

[15] Teng L, Li H, Yin S, Sun Y. A Modified Advanced Encryption Standard for Data Security. *International Journal of Network Security*, 22(1):112–117, 2020.

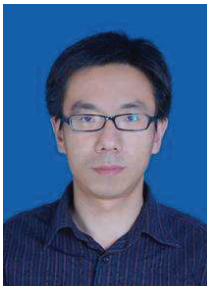
[16] More P R, and Gaikwad S Y. An Advanced Mechanism for Secure Data Sharing in Cloud Computing using Revocable Storage Identity Based Encryption. *International Journal of Engineering Business Management*, 1(1):12–14, 2017.

[17] Paka T, and Divya S. Data Storage Security and Privacy in Mobile Cloud Computing Using Hierarchical Attribute Based Encryption (HABE). *International Journal of Computer Sciences and Engineering*, 7(6):750–754, 2019.

[18] Alshammari A S. A Novel Cryptosystem based on Chaotic Signals for Data Encryption Applications and CDMA Communication System. *Przeglad Elektrotechniczny*, 98(2):10–13, 2022.

[19] Kulshrestha V, Verma S, and Krishna C R. Hybrid probabilistic triple encryption approach for data security in cloud computing. *International Journal of Advanced Intelligence Paradigms*, 21(1/2):158–173, 2022.

Biographies



Dongliang Bian, born in July 1977, in Baoding, Hebei Province, graduated from the school of economics, Hebei University, with a bachelor's degree in 1998. He is now an associate professor of Baoding vocational and technical college. His research interests include vocational education and web front-end development. He has won the third prize in the provincial vocational college skills competition, published five academic papers, participated in one textbook of the 12th Five Year Plan, presided over and participated in two provincial and municipal projects.

Jun Pan, born in November, 1981, in Baoding, Hebei Province, graduated from Hebei Agricultural University with a bachelor's degree in computer science and technology in 2005 and obtained a master's degree in engineering from Hebei University in 2011. He is now an associate professor of Baoding Vocational and Technical College and a special commissioner for science and technology in Hebei Province. He has obtained red hat RHCE certification and rhci certification as lecturer. His research interests are vocational education and computer network technology. He has guided students to participate in the national vocational college skills competition and won one second

prize and two third prizes. He has published six academic papers, edited four textbooks, presided over two municipal projects, and participated in two provincial and municipal projects.

Yanhui Wang, born in December, 1980, graduated from Hebei University with a master of Engineering in 2012, and is now an associate professor of Baoding Vocational and Technical College. His research interests are computer technology, vocational education, and e-commerce. He has published six academic papers, edited two textbooks, presided over three provincial and municipal projects, and won one third prize for provincial teaching achievements.