Safety Protection of E-Commerce Logistics Information Data under the Background of Big Data

Yuan Zhao[1] and Yanyan Zhang[2]
(Corresponding author: Yuan Zhao)
School of Business Administration, Shandong Women's University[1]
No. 2399, Daxue Road, Changqing district, Jinan, 250300, China
(Email: yuanzhsdwu@yeah.net)
School of Economy, Shandong Women's University, Ji'nan, Shandong 250300, China[2]
(Received May 31, 2018; revised and accepted Sept. 22, 2018)

Abstract

E-commerce logistics information data during transmission on the Internet are easy to be maliciously tampered; hence, effective measures are needed to protect them. In this paper, technologies of identity authentication and digital encryption in a logistics information system were studied. The data encryption technology based on RSA algorithm and identity authentication technology based on Certificate Authority (CA) certification system were proposed. The results demonstrated that RSA algorithm based technology had higher security and was not easier to crack between both technologies; the identity safety of transactions of both technologies could be identified through CA certificate and digital signature. Finally, some suggestions were put forward for ensuring the safety of logistics information.

Keywords: Big Data; Data Encryption; E-Commerce; Information Security; Logistic Information

1 Introduction

Network security has attracted more and more attention [1, 12, 27]. In the era of big data, information security has been more seriously threatened [14, 24]. E-commerce development rapidly relies on the Internet, and e-commerce logistics information data also explosively increase with the development of e-commerce. The massive data are easy to be attacked and damaged because of network security problems when they are transmitted; therefore, Information security is the basis for ensuring the sound development of e-commerce [8, 15]. Therefore, how to effectively protect these logistics information data has become the key to the development of e-commerce.

In a study of Huang [7], Radio Frequency Identification (RFID) [4, 11, 22, 23] based logistics information system analyzed was found that when combined with Internet technologies, it could realize tracking and sharing of data, so its security risks could be reduced through measures such as authentication protocol and data encryption. Zhang *et al.* [26] put forward a logistics information protection system based on encrypted quick response (QR) code. By means of sectional encryption, the logistics information was stored in QR code, which can protect personal privacy information under the premise of reasonable logistics business. Gao *et al.* [5] considered that mobile authentication devices used by logistics enterprises could also affect the security of logistics information and then proposed a method to protect logistics information by attribute-based encryption and location-based key exchange. This method could access the location and attributes of mobile devices and meet the requirements of information protection.

In this study, RSA-based data encryption technology and certificate authority (CA)-based identity authentication technology were used in a logistics information system to control the transmission of logistics information and the access of users to prevent information leakage, and put forward some measures to protect logistics information.

2 Big Data and E-Commerce Logistics Information

2.1 E-Commerce Logistics Information under the Background of Big Data

With the development of network and information technology, e-commerce has been gradually rising and widely praised. The biggest advantage of e-commerce is shortening transaction time and improving transaction efficiency. Logistics is the last link of e-commerce, which has an important impact on the success or failure of transactions.

Logistics information contains a lot of valuable information, such as customer name, address, contact information, etc.; therefore, it is an important asset of enterprises [17]. The information exchange between E-commerce and logistics enterprises is carried out through the network. The establishment of a logistics system is based on the Internet, so the information on the network is vulnerable to attacking and leakage [21]. The problem of network security is very serious. In the era of big data, logistics information data is growing rapidly, and massive information data concentrate; therefore, it is difficult to manage and protect them effectively, which brings opportunities to hackers. Logistics information is facing many security problems.

2.2 Security Problems of Logistics Information Systems

The development of network technology increases risks of information security [18]. E-commerce logistics information system relies greatly on the network. But the problem of network security has become more and more serious because the high openness and freedom of network are mainly reflected on:

1) Information security. Effective information of users can be got through illegal interception when logistics information is transmitted in the network. The leakage of private information of users can have a large impact on the credit of e-commerce enterprises and logistics enterprises. In addition, logistics information may be maliciously tampered or deleted in the transmission process, resulting in incomplete information and affecting the normal transactions of users.

2) Virus. Network is the best medium for virus transmission. Logistics information is easy to be attacked by viruses when being transmitted in the network, which will not only affect the transmission of logistics information, but also affect a larger area after further transmission.

3) Identity uncertainty. E-commerce completes transactions on a virtual platform, and the identity of both parties is uncertain. Illegal elements may embezzle the legitimate information of users for transactions through illegal means.

E-commerce logistics information is easy to be intercepted, tampered and embezzled in the transmission process, which brings huge losses to e-commerce enterprises, logistics enterprises and users. Therefore, it is necessary to pay more attention to logistics information security and strengthen the security protection of logistics information systems. The security protection measures of logistics information systems include identity authentication, data encryption, digital signature, certificate management and security maintenance. This study focuses on the identity authentication technology and data encryption technology.

3 Identity Authentication Technology

3.1 Identity Authentication

Authentication means that the user proves the reliability of his or her identity by some way. Authentication means that both parties in the electronic commerce need to confirm each other's identity before they have a conversation, that is, key exchange. In the process of key exchange [3, 13], in order to prevent identity impersonation and information leakage, it is necessary to make important information transmitted as a ciphertext through private key and public key.

3.2 CA Identity Certification

CA identity certification can be applied in a large-scale network environment. The system can issue different levels of digital certificates for different types of users such as institutions, servers or individuals. It has been widely used in many fields such as electronic banking, electronic shopping malls and bank-enterprise reconciliation. The system can ensure the security of identity authentication [9, 10].

Identity authentication includes certificate authentication and digital signature authentication. The specific process is as follows:

1) Security certificates and signatures are sent to the server of the logistics information system from the client end and then transmitted after being encrypted by the public key.

2) The logistics information system receives the client information, uses the private key to verify the obtained certificate and signature, obtains the customer's public key from the certificate after confirming the validity, and then completes the client authentication through the client's public key. Next, the logistics information system uses the private key to complete the signature of the system certificate, and then the certificate and signature are transmitted to the client through the client public key.

3) After receiving the information of the logistics information system, the client first decrypts the information through the private key, confirms the validity of the certificate and signature, and then decrypts the signature through the public key of the logistics information system. The process of identity certification is shown in Figure 1.

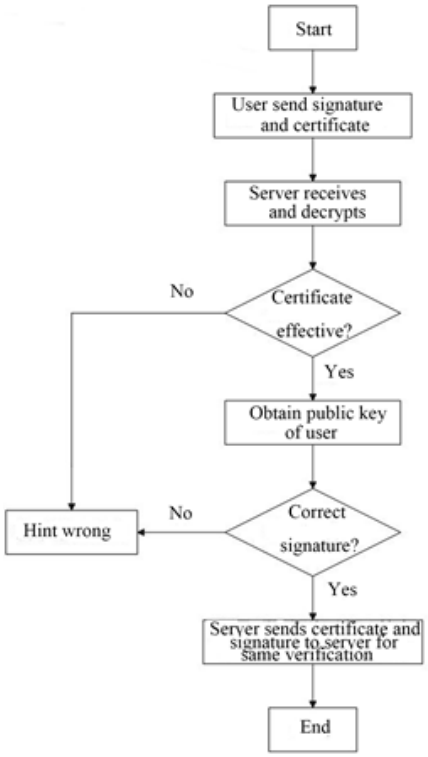

Figure 1: The procedures of identity certification

4 Data Encryption Technique

4.1 Data Encryption

Data encryption refers to re-encoding the logistics information transmitted in the network in some way, hiding the information content in the data encoding, and storing and transmitting the information in an unreadable form [16]. When data is encrypted, hackers cannot obtain the real content of the information. After the information is encrypted, the receiver needs to decrypt the data using decryption key. The keys are the conversion keys between the plaintext and the ciphertext, including encryption and decryption keys. The process of information encryption and decryption is shown in Figure 2.

The encryption and decryption process of information can be expressed by formulas. The encryption process can be expressed as $S = A(M)$, and decryption process can be expressed as $M = C(S)$, where M stands for plaintext, S stands for ciphertext, A stands for encryption algorithm, and C stands for decryption algorithm. The plaintext can be obtained by $C(A(M)) = C(S) = M$.

4.2 RSA Encryption Algorithm

RSA encryption algorithm is a commonly-used excellent public-key encryption algorithm [2, 19]. Its principle is prime factorization of large integer [20].

A key is needed before RSA encryption. The process of obtaining the key is as follows.

1) Two large integers, m and n, were selected and kept secret.

2) Calculate mode $X = m \times n$ and $H(X) = (m-1) \times (n-1)$, where H refers to Euler function, X is public, and $H(X)$ is private.

3) An integer p was selected $(1 < p < H(X))$, and p and $H(X)$ are relatively prime; moreover, p is private.

4) Calculate the multiplicative inverse q of p, and q is private.

5) Delete m, n and $H(X)$, and public key (p, x) and private key (q, x) are obtained.

When RSA algorithm is used in data encryption, data needs to be segmented to make the length of every group of data smaller than X. Then plaintext M is encrypted as ciphertext S:

$$S = M^p \bmod X.$$

The decryption process is $M = S^q \bmod X$.

Suppose user A needs to send a fragment of information M to user B. The public and private keys of A are (p_1, X_1) and (q_1, X_1), respectively, and the public and private keys of B are (p_2, X_2) and (q_2, X_2), respectively.

Encryption: Plaintext d_m is input, and its length was made to be smaller than X. It is encrypted using the public key of B. Ciphertext S is obtained as follows:

$$S = M^{p_1} \bmod X_2.$$

Decryption: After B receives the ciphertext, B decrypts it using the private key of B. Plaintext M is obtained as follows:

$$M = S^{q_2} \bmod X_2.$$

Digital Signature and Verification: Plaintext d_m is input and signed using the private key of A. Then the output plaintext is d_p:

$$d_p = M^{p_1} \bmod X_1.$$

After B receives the signed text d_m, it is decrypted using the public key of A. Finally plaintext $d_m = S^{q_1} \bmod X_1$ is obtained.

4.3 Security Verification of RSA

In the actual application of RSA algorithm, m and n are usually more than 100 bits, which increases the breaking difficulty. Suppose that a computer can make 100 million of operation in one second, then the operation time of RSA algorithm under different bits is shown in Table 1.

It can be found from Table 1 that the longer the length of key, the more complex RSA operation. It indicates that RSA algorithm with a length of key longer than 100 bits is absolutely safe and impossible to be broken.

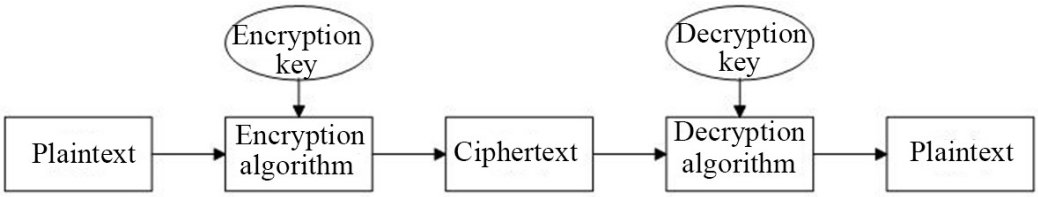

Figure 2: The encryption and decryption of information

Table 1: The operation time of RSA

Decimal digit	50	100	300	500
Operation times of decomposition factor	1.4×10^8	2.3×10^{13}	1.5×10^{27}	1.3×10^{37}
Operation time of decomposition factor	2.4 min	270 days	4.9×10^{13} days	4.2×10^{23} days

The use of RSA algorithm can encrypt the logistic information of e-commerce such as the name, address and telephone number of both transaction parties. Table 2 shows the results of some logistics information after being encrypted by RSA public key.

It can be found from Table 2 that the logistics information data become unidentifiable character string after being encrypted by RSA. Decryption with the key is necessary; otherwise, they look like ineffective character strings. Even if logistics information data is intercepted, it cannot be decrypted without corresponding keys, which ensures the security of logistics information data in the process of transmission.

5 Security Protection Measures Of Logistics Information Data

5.1 Strengthening the Establishment of Logistics Information Systems

Relevant government departments need to strengthen the guidance for the scientific construction of logistics information systems, help enterprises to establish a sense of logistics information protection, establish a safe and effective logistics information system, actively promote the exchange and circulation of advanced logistics information protection technology, improve and strictly protect the relevant laws and regulations of logistics information, and strengthen access control and transmission control of logistics information systems [6]. Research and promotion efforts on the core technology of logistics information systems, such as identity authentication and data encryption, need to be strengthened to avoid information leakage to achieve logistics information security management.

5.2 Realizing Safety Storage of Logistics Information

E-commerce enterprises and logistics enterprises should fully realize the importance of logistics information data for the development of enterprises in the era of big data, and improve the attention to logistics information management. For massive logistics information, enterprises need to properly preserve them, so as to avoid huge losses brought by information leakage. Distributed file system technology can be used to realize the cloud-based security storage of logistics information data and backup extremely important core data. In addition, enterprises can set access permission to avoid malicious steal of information and ensure security of logistics information.

5.3 Improving the Protection Technology of Logistics Network

The development of the Internet has improved the efficiency of logistics and also brought challenges to information security [25]. The safety of logistics network cannot be ignored. In order to avoid external attacks on the logistics network, it is necessary to take certain technical measures to establish protection measures and hide the internal network channels. The core network can be isolated by physical isolation technology and firewall isolation technology. Enterprise technicians need to strengthen the research on logistics network protection technology to ensure that the internal information of the enterprise will not be leaked.

6 Conclusion

With the development of Internet technology, network security becomes more and more serious. E-commerce logistics information is easily attacked by criminals because it can be disseminated through the Internet. In this paper, data encryption technology and identity authentica-

Table 2: RSA encryption result

Plaintext	Ciphertext
Zhao Xiaolan	r102yc/tKB+kE5RCpZbCSqmUdpFZj4Oq3Ct4sVCZnCofbPlJ/+vit/fZe6AkiqI3vZbLs7zha qzUioa0TsPkML7A9wnpZlS9LcqM6it7Igy+KQPC0BhpTG89eFhoS7ZVII6ITxL8Igoopzvx2 S/tnTqgN+8QaT6iKRqMoL7LyoY=
250000	QdjyxP1L/D7B3L3q8PhabLrjg9yxY/vCoVh+und+PipCOXjI5/5Znxom0Hr3bAiIyevdzFP HFVkfEK9c8tqKuB7ThKQ67HIVXyXjA6WsvBnn+RM6yBqPXRe/9pjgZt2kND0hm4NAZ V4pitCk7sImsAw0os4X9S+axQuYvJ4uG0s=
Shandong Women's University in Jinan	eU+++6415N6+40YSY1Jq5JqTRdLgg5wCrP2DV53asz73Jt9aNVfLYcbpTDaDLbrfeO8Oz 2oV5NsBr+frI9GXw1Stk5T7Pq+MV4dIdZlh4KB+m79iwAJnbXerINVBH8dipe6pW3xTiV B4kB0/ctBQBXgixmhcIYXG5waERzKzZcE=
Shandong province	Ldc0kZZ1t7MAclJ1xZBjWddNsDZouiW60hhNzTknGVzwTqT15eNA5c7+2Bcq/cKdbamk isarQns7u3+bkBJTSmOyx95ZreRN5m8GYgGc4Z7K+RG2vJoP1FegGW5XuHh9Ne1/a+ LLEmCBtYeiVDTSiu3YHnVCnWR1pO4rXCstSaY=

tion technology in logistics information system were studied. RSA algorithm was proposed and CA authentication system was used for identity authentication. These two technologies can effectively improve the security of logistics information. The advantages of e-commerce industry need reliable and efficient logistics to guarantee security; therefore, only when the safety of logistics information data is ensured, e-commerce can develop safely.

References

[1] A. A. Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116–123, 2017.

[2] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[4] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255–259, 2007.

[5] Q. Gao, J. Zhang, J. Ma, *et al.*, "LIP-PA: A logistics information privacy protection scheme with position and attribute-based access control on mobile devices," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9436120, 14 pages, 2018. (`https://doi.org/10.1155/2018/9436120`)

[6] D. Geng, X. Li, H. Liu, "Research on the network security of a E-commerce system based on logistics information platform," in *IEEE International Conference on Computer and Communication Technologies in Agriculture Engineering*, pp. 24–27, 2010.

[7] K. Huang, "IIPM as a solution to the security problems of RFID-based logistics information system," in *International Conference of Logistics Engineering and Management*, pp. 2367–2371, 2010.

[8] M. S. Hwang, C. T. Li, J. J. Shen, Y. P. Chu, "Challenges in e-government and security of information", *Information & Security: An International Journal*, vol. 15, no. 1, pp. 9–20, 2004.

[9] M. S. Hwang, L. H. Li, "A new remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[10] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[11] M. S. Hwang, C. H. Wei, C. Y. Lee, "Privacy and security requirements for RFID applications", *Journal of Computers*, vol. 20, no. 3, pp. 55–60, Oct. 2009.

[12] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[13] I. C. Lin, M. S. Hwang, C. C. Chang, "A new key assignment scheme for enforcing complicated access control policies in hierarchy", *Future Generation Computer Systems*, vol. 19, no. 4, pp. 457–462, May 2003.

[14] L. Liu, Z. Cao, C. Mao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[15] G. Lv, M. Gao, X. Ji, "Research on information security of electronic commerce logistics system," in *International Conference on Intelligent Computing*, pp. 600–611, 2016.

[16] R. Sailaja, C. Rupa, A. S. N. Chakravarthy, "Intensifying the security of information by the fusion of random substitution technique and enhanced DES,"

in *Smart Computing and Informatics*, pp. 487-496, 2017.

[17] A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57(C), pp. 14–30, 2016.

[18] Z. A. Soomro, M. H. Shah, J. Ahmed, "Information security management needs more holistic approach: A literature review," *International Journal of Information Management*, vol. 36, no. 2, pp. 215–225, 2016.

[19] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[20] F. T. Wang, T. W. Lin, H. F. Tsai, *et al.*, "Applying RSA signature scheme to enhance information security for RFID based power meter system," in *International Conference on Information Engineering*, pp. 549–556, 2014.

[21] L. Wang, T. Su, "A personal information protection mechanism based on ciphertext centralized control in logistics informatization," in *LISS 2013*, pp. 1207–1212, 2015.

[22] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[23] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[24] L, Xu, C. Jiang, J. Wang, *et al.*, "Information security in big data: privacy and data mining," *IEEE Access*, vol. 2, no. 2, pp. 1149–1176, 2017.

[25] J. Zhang, L. Ye, "The Internet of Things and Personal Privacy Protection," in *International Conference of Logistics Engineering and Management*, pp. 2892–2898, 2010.

[26] X. Zhang, H. Li, Y. Yang, *et al.*, "LIPPS: Logistics information privacy protection system based on encrypted QR code," in *IEEE Trustcom/BigDataSE/ISPA*, pp. 996–1000, 2016.

[27] S. Zhong, Z. Deng, "Model design of information security monitoring system of nanchang bonded logistics park," in *IEEE International Symposium on Information Science & Engineering*, pp. 489–493, 2010.

Biography

Zhao Yuan, born in January 17, 1986, is a graduate student and a professional teacher at Shangdong Women's University. Her research direction is electronic commerce and international logistics. Since December 2015, she has worked at Shangdong Women's University. In 2016, she chaired a youth project at the school level. A paper was published in 2016 and was searched by ISSHP. Three papers were published in 2017.

Zhang Yanyan, born in December 21, 1986, is a graduate student and a professional teacher at Shangdong women's university. The research direction is economy and finance. From August 2013 to November 2014, she worked in Jinan Branch of China Post Savings Bank. Since December 2014, she has worked in Shangdong women's university. In 2015, she chaired a youth project at the school level. In 2017, she presided over a project of Shandong Youth Quality Education Base, in 2018 she presided over a project of Shandong Youth Education Science Planning, and published 8 academic papers from 2015 to 2018.