Volume 9 Issue 4, 2023
DOI: 10.6919/ICJE.202304_9(4).0034

Online Shopping Information Encryption based on Hierarchical Encryption Model

Chuanqi Ma

School of Civil Engineering and Transportation, South China University of Technology, Guangzhou, Guangdong, 510641, China

202064200390@mail.scut.edu.cn

Abstract

With the continuous development of information technology, online shopping has become a preferred way of shopping by its convenience and rapidity. However, online shopping also brings some hidden dangers to consumers while serving them. The personal information provided by consumers in shopping becomes a commodity and is used by businesses, which seriously threatens the balance of consumers' rights and interests and the market. At present, for many large enterprises, most online shopping data are processed in batches in a unified encryption mode, which leads to an imbalance between efficiency and security. Therefore, this paper proposes a layered encryption model. By adopting different encryption algorithms for various types of data generated in the online shopping process, it can not only improve the efficiency and security of encryption on the premise of ensuring security, but also can guarantee the interests of enterprises and protect the personal information of consumers to the greatest extent. The experiment shows that the simulation results of the model achieve high accuracy under the premise of ensuring data encryption.

Keywords

Online Shopping; Personal Information Security; Hierarchical Encryption Model; Encryption Algorithm.

1. Research Background

1.1 Research Objective

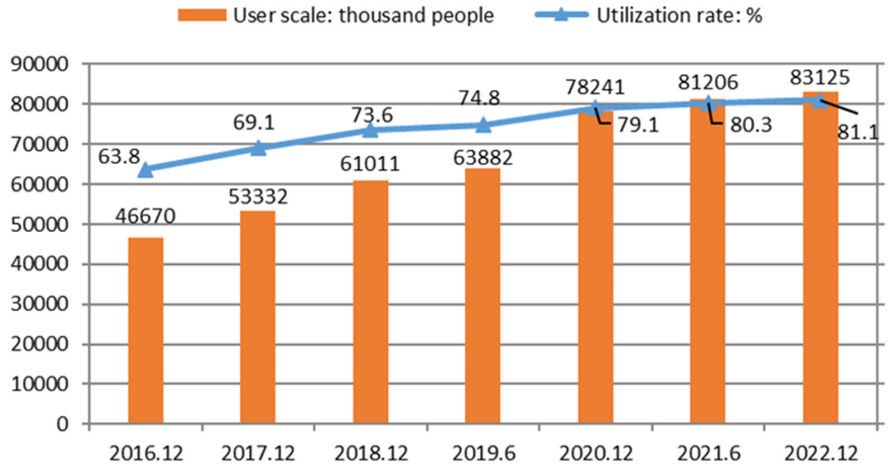


Figure 1. Statistics of China's online shopping scale

Nowadays, online shopping[1] is becoming increasingly popular and has a large development market. Figure 1 illustrates the development trend of online shopping. Take China as an example, the user base of online shopping is large, showing a continuous upward trend. Therefore, there are many online shopping data generated. However, the current information protection for consumers is not comprehensive[2]. There is also a lack of mature regulatory system at the legal level, which makes it possible for illegal businesses to take advantage of it, and the infringement of personal information is becoming more and more serious. Due to the relatively large amount of personal information generated in online shopping, but the necessary information in different links is limited, this paper is committed to improving the protection mechanism from the information source, using different encryption algorithms for different links of online shopping, and providing only the necessary information of the business, to better ensure the security of personal information.

1.2 Research Status

The current data encryption is mainly divided into symmetric encryption and asymmetric encryption[3]. The key difference is whether the encryption and decryption keys are the same. Symmetrical encryption has higher encryption efficiency but lower security. Asymmetric encryption is more secure, but it has defects in processing speed. At present, the mainstream encryption algorithms are as follows:

For symmetric encryption, Caesar cipher is achieved by moving letters in the alphabet to a certain position[4]. At present, it is mainly used for text encryption in combination with matrix mixed permutation. DES (Data Encryption Standard) is an encryption standard with a 64-bit key, which is widely used in bank outreach services and database secondary key design[5]. AES (Advanced Encryption Standard) is a new generation of 128-bit key encryption standard designed to replace DES, which is mostly used for encryption of electronic information systems[6]; For asymmetric encryption, RSA is one of the most widely used encryption algorithms that has been included in the ISO international standard, mainly used in QR codes[7].

2. Introduction to Relevant Theories and Technologies

2.1 Online Shopping Information

Compared with the personal information generated by traditional offline shopping, the personal information involved in online shopping is more extensive and easy to collect [8]. Specifically, it includes: consumer name, consumer gender, consumer age, consumer ID number, consumer communication method, product delivery address and other traditional purchase information. It also includes information indirectly generated by consumers in the online process, including interests, financial status, shopping time, etc.

2.2 Online Shopping Process

The online shopping process can be divided into online and offline stages[9]. In the online stage, the e-commerce platform is used as the guarantee platform for transactions, and the platform needs to retain all information of consumers. For the merchants who enter the platform, they need the name, communication method and product delivery address of the consumer to send the goods. In the offline stage, the goods will be transported to the logistics concentration point first. Due to the need of checking the transportation process, it needs to know the name, gender and communication method of the consumer. Then the goods are delivered to the consumers through the courier. The courier needs to master the name, communication method and product delivery address information of the consumers during the delivery and verification process.

2.3 Hierarchical Encryption Model

The layered encryption model is divided into three layers. Each layer uses different encryption algorithms according to the properties of information. The first layer uses Caesar Cipher for symmetric encryption, which is mainly used to encrypt the consumer's name, address and contact information data. This type of data is commonly necessary for online sales and offline distribution, so it uses a relatively simple encryption form; The second layer uses AES algorithm for symmetric encryption, which is used to encrypt consumer gender, age and consumption time data. This type of data is generally used to resolve disputes arising from the consumption process. It is very useful and highly private data. Its key is only available to the post-sale department of the e-commerce platform and offline distribution point; The third layer uses RSA algorithm asymmetric encryption, which is used to encrypt the data related to the quantity and content of purchased goods. Such data involves the important privacy of consumers and is the basis for illegal merchants to push advertisements. Therefore, the encryption mode with the highest security is used to strictly prevent the disclosure of such information. Figure 2 shows the hierarchical model proposed in this paper.

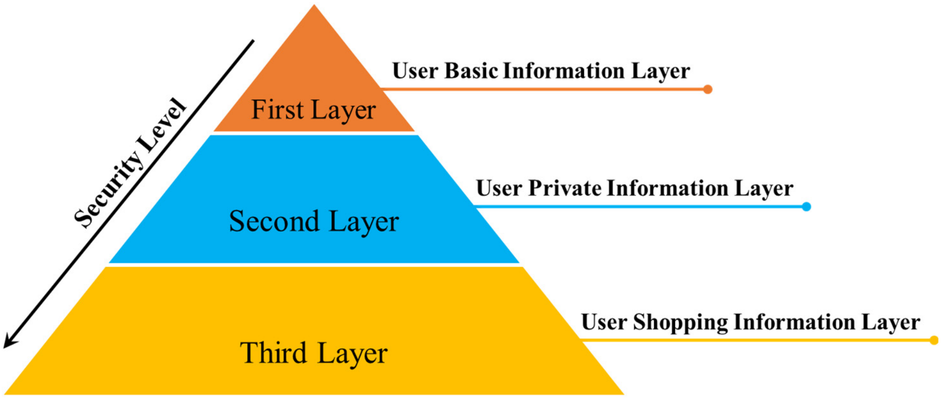

Security Level
First Layer
Second Layer
Third Layer
User Basic Information Layer
User Private Information Layer
User Shopping Information Layer

Figure 2. Topological Structure of Hierarchical Encryption Model

Table 1 shows the encryption details of the hierarchical model.

Table 1. Layered encryption model design table

Layer	Encryption Algorithm	Information Type	Security level
User Basic Information Layer	Caesar Cipher	Consumer's name and address	Low
User Private Information Layer	AES	Consumer's age and gender	Medium
User Shopping Information Layer	RSA	Name and quantity of goods	High

3. Experiment

3.1 Experimental Indicators

The encryption efficiency of different layers is expressed by the quotient of encryption time and the size of encrypted information. The calculation formula is:

$$Efficiency = Time\_cost/Size \tag{1}$$

Where, $Efficiency$ represents the efficiency of encryption; $Time\_cost$ represents the time used for encryption, in ms; $Size$ indicates the size of encrypted information, in Bytes.

3.2 Experimental Design

The user's basic information layer uses Caesar cipher to encrypt the data. Take consumers' name information as an example. The encryption is shown in Table 2.

The user's private information layer uses AES to encrypt data. The encrypted information takes the shopping time, sex and age of the consumer as an example. The encryption is shown in Table 3.

Table 2. Cryptographic Information of Caesar Cipher

Plaintext	Key	Ciphertext	Efficiency
Clement Haywood	16	Sbucudj Xqomeet	0.13
Werner Ernest	18	Owjfwj Wjfwkl	0.23
Will Charles	7	Dpss Johyslz	0.17

Table 3. AES Encrypted Information

Plaintext	Ciphertext	Efficiency
2023.1.8 18:27 Male 24	?�s������Zg�1�⍰Z�F⍰⍰YD⍰⍰)9z	5
2022.11.11 9:00 Female 50	`E!⍰(⍰Ű\⍰P⍰⍰⍰⍰⍰⍰⍰⍰⍰x⍰⍰⍰⍰ 8�⍰G_	4
2022.5.1 21:30 Female 32	R⍰⍰%dW7⍰⍰⍰H2⍰⍰⍰B⍰}⍰⍰⍰MY⍰WU⍰d⍰t⍰⍰	5

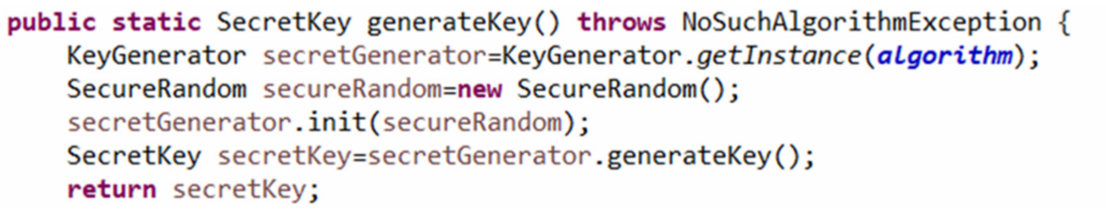
The user's shopping information layer uses RSA to encrypt the data. The encrypted information takes the consumer's shopping information and quantity as an example. The encryption is shown in Table 4.

Table 4. RSA Encrypted Information

Plaintext	Ciphertext	Public Key	Privat Key	Efficiency
Avieta Waffle 70g×16	SW49xA…wQihPxFNqI	MIGfMG…Mayo0wIDAQAB	MIICdwIN…itwpm7rxh2QKcU	10
Bayaspirin 300mg	gWMi3k…Ds85jVGCLp4	MIGfMAw…O90J6wIDAQAB	MIICdQI…ANBgkwYloy6-zHjJ3	13
Nike socks 2 pairs	A1aVJH…MVB3XL1jU	MIGfMA0G…wIDAQAB	MIICdwIBA…07ff-1uwagc4	11

3.3 Method Design

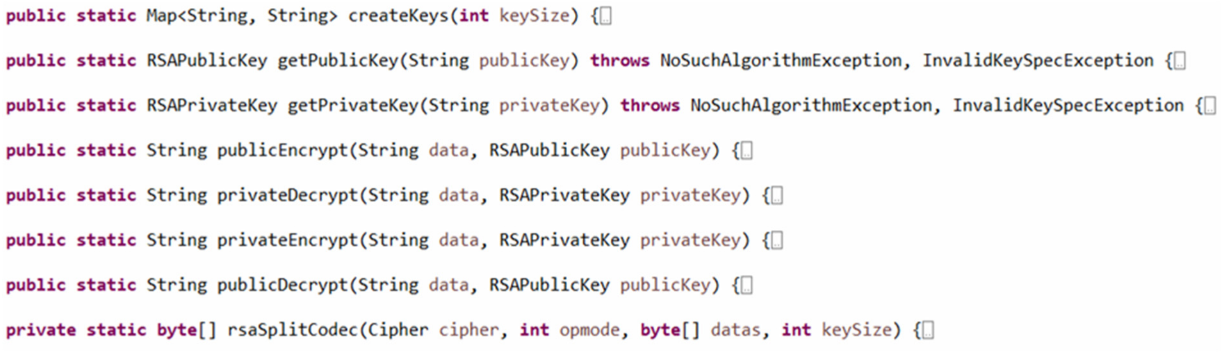
AES uses three methods. The first method is called generateKey, which is used to generate and output the secretKey exclusive to the encrypted information. The second method is called encrypt, which is used for information encryption. Enter the plaintext called content and secretKey, then output the encrypted ciphertext called encryptResult. The last method is decrypt, which is used for information decryption. Enter the encrypted information called encryptResult and secretKey, then output the decrypted plaintext called decryptResult. Taking method 1 as an example, the code design is shown in Figure 3, and the key generation function is implemented.



```
public static SecretKey generateKey() throws NoSuchAlgorithmException {
    KeyGenerator secretGenerator=KeyGenerator.getInstance(algorithm);
    SecureRandom secureRandom=new SecureRandom();
    secretGenerator.init(secureRandom);
    SecretKey secretKey=secretGenerator.generateKey();
    return secretKey;
```

Figure 3. Key generation code design

RSA uses seven methods in total. The first method is called getPublicKey. This method obtains PublicKey through X509 encoded Key instruction. The second method is called getPrivateKey. This method obtains the PrivateKey through the Key instruction encoded by PKCS # 8. The third method, named publicEncrypt, is used for public key encryption. The input PublicKey is encrypted to RSAPublicKey and output. The fourth method, named publicDecrypt, is used to decrypt the public key, decrypt the input RSAPublicKey to PublicKey and output it. The fifth method is called privateEncrypt, which is used for private key encryption. The input PrivateKey is encrypted to RSAPrivateKey and output. The sixth method is called privateDecrypt, which is used to decrypt the private key. The input RSAPrivateKey is decrypted to PrivateKey and output. The last method is called rsaSplitCodec, which is used for cutting and decoding. The overall structure of the method is shown in Figure 4.



```
public static Map<String, String> createKeys(int keySize) {□

public static RSAPublicKey getPublicKey(String publicKey) throws NoSuchAlgorithmException, InvalidKeySpecException {□

public static RSAPrivateKey getPrivateKey(String privateKey) throws NoSuchAlgorithmException, InvalidKeySpecException {□

public static String publicEncrypt(String data, RSAPublicKey publicKey) {□

public static String privateDecrypt(String data, RSAPrivateKey privateKey) {□

public static String privateEncrypt(String data, RSAPrivateKey privateKey) {□

public static String publicDecrypt(String data, RSAPublicKey publicKey) {□

private static byte[] rsaSplitCodec(Cipher cipher, int opmode, byte[] datas, int keySize) {□
```

Figure 4. RSA code structure

3.4 Experimental Analysis

In the first layer of the model, when encrypting the consumer's name information, Caesar's password randomly generates the key 16, that is, the offset is 16, and the plaintext Clement Haywood is encrypted into the ciphertext Sbucudj Xqomet. The encryption process is simple, but the efficiency is low, only 0.13. Because the data encrypted at this layer is mostly repetitive and common data, it can meet the encryption requirements; In the second layer of the model, AES encrypts the plaintext 2023.1.8 18:27 Male 24 into ciphertext ?�s������Zg�1�□Z�F□□YD□□)9z when encrypting the consumption time, consumer's sex and age information. The data encrypted in the second layer has the characteristics of large data volume and low repeatability, and the encryption efficiency of this process reaches 5, close to 50 times of that of the first layer, which can give good consideration to the encryption efficiency and security; In the third layer of the model, when encrypting the shopping information and quantity information, RSA targeted the plaintext Avieta Waffle 70g × 16 Encrypt as ciphertext SW49xA... wQihPxFNqI, at the same time generate the public key MIGfMG... Mayo0wIDAQAB and the private key MIICdwIN... itwpm7rxh2QKcU. They need to cooperate to achieve decryption. The security and efficiency of encryption in this layer are the highest among the three layers, reaching 10, which conforms to the characteristics of its encrypted data.

4. Conclusion

To sum up, in today's prevalence of online shopping, the contradiction caused by consumer personal information disclosure is becoming increasingly prominent, so it is particularly important to protect consumer information security. The core content of this article is to encrypt the personal information generated during the whole online shopping process. Based on the current unified encryption, a layered encryption model is innovatively proposed. The simulation results show that the model can ensure the security of online shopping information while taking into account the encryption efficiency. It also has strong practicability. At the same time, the model can provide some reference for information encryption in other fields. In future practical applications, the encryption algorithm in the model can be appropriately replaced for encryption under different circumstances, so as to better complete the encryption work.

References

[1] Zhao, J. (2011). The e-business development trends in china online shopping industry. In: 2011 International Conference on Computer Science and Education. Qingdao. 537-547.

[2] Chen, J., Xie, X., & Jing, F. (2011). The security of shopping online. In: 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. Harbin. 9: 4693-4696.

[3] Li, W. (2022). Data encryption technology in computer network information security. Network Security Technology and Application, 11:23-24.

[4] Yu, X., & Yu L. (2013). Research on a data cryptography algorithm based on Caesar ciphering. Computer Security, 04: 57-60.

[5] Xu, H., & Li, Y. (2009). Application of DES encryption algorithm in protecting data security in file transmission. Net info Security, 06:24-26+76.

[6] Guo, G., Qian, Q., & Zhang, R. (2015). Different implementations of AES cryptographic algorithm. In: 12th IEEE International Conference on Embedded Software and Systems. New York. 1848-1853.

[7] Yu, Z. (2018). Application research of RSA algorithm in two-dimensional code anti-counterfeiting technology. Network Security Technology and Application, 09:39+21.

[8] Jin, J. (2022). Research on the protection of personal information of online shopping consumers Master's thesis of Hebei University of Economics and Trade, 7: 50.

[9] Chen, Y., Feng, G., & Ren L. (2021). Research on the impact of online and offline interactive experience on consumers' purchase intention under the new retail background. Productivity Research, 02:99-104.