Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 9, No. 3, 2023

A Layered Encryption Model PABB Based on User Privacy in E-commerce Platforms

Jingwu Wen[1, *]

[1]Faculty of Geosciences and Environment Engineering, School of Southwest Jiaotong University, Chengdu, Sichuan 610031, China
[*] Corresponding author: vincentwen@my.swjtu.edu.cn

Abstract: In the era of big data, e-commerce platforms have increasingly strict requirements for encryption systems to prevent user privacy breaches. Traditional encryption systems use a single encryption algorithm, which cannot achieve a balance between efficiency and security. The layered encryption model PABB classifies and layers user data of different security levels, using targeted different encryption algorithms for protection, balancing the requirements of security and efficiency.

Keywords: E-commerce, Personal privacy, Hierarchical model, Encryption algorithm.

1. Introduction

E-commerce is diverse, and people give slightly different definitions according to different angles. From the perspective of the Internet, e-commerce is described as various business activities carried out through the Internet, including advertising, trading, payments, services and other activities. [1] However, this definition has its limitations, because e-commerce is not restricted to the Internet. From the perspective of economics, e-commerce is a business transaction between enterprises, enterprises and consumers that takes place on the open network. It is based on digital data processing and transmission process including multimedia, including all transaction forms related to business activities.[2] This definition limits the identity of e-commerce participants and the way of transaction. Later, it was defined as the completion of any form of business transaction between participants by electronic means rather than physical exchange or direct physical contact.[3] From the perspective of electronization, e-commerce is to realize the electronization of the whole trade activity.[4] Now, e-commerce refers to all business activities of enterprises through the Internet. With the popularity of smart phones, more and more business practitioners or non-practitioners of ordinary people also participate in mobile e-commerce activities through e-commerce platforms. Through the e-commerce platform, users can trade goods in kind, services, information and other goods.

Although e-commerce makes shopping more convenient for modern people, because e-commerce platform will bind a series of privacy information such as user name, contact information, address, bank card, etc., once the platform is vulnerable or the privacy data is not protected, it will cause a series of serious privacy security problems.

Personal privacy generally refers to personal information, activities, fields, etc. that citizens are unwilling to disclose to others.[5] In e-commerce activities, first, users need to submit a large amount of privacy information to the platform, including capital account and its password, platform login account and its password, user's personal name, ID number, receiving address, etc; The second is to record the behavior of users during the use of e-commerce platforms' apps or web pages. This article provides the following definition for user privacy in e-commerce activities. There are two types of personal privacy in e-commerce: information that users upload to the platform but do not want to disclose, and records that users leave behind during platform activities and do not want to disclose.Up to now, researchers have taken such methods as symmetric key encryption, asymmetric key encryption, database encryption to protect user privacy data, which has solved a series of problems such as user data being easy to be cracked and leaked. Based on the importance of protecting personal information security under big data, this paper proposes a layered encryption model PABB for personal information recorded/stored on e-commerce platforms. From top to bottom, the security level is user payment information layer, user account information layer, user behavior information layer, and user basic information layer. We found that many e-commerce platforms did not encrypt all users' private information in a timely manner, which led to the fact that when there was an information disclosure event, the hackers could directly use the stolen original data for transactions or other criminal activities. The layered encryption model reasonably layers the existing user data according to the requirements of different information use frequency on the time complexity of the encryption algorithm and the requirements of different information on the security of the encryption algorithm. Different encryption algorithms are used according to the requirements of different levels on the security and efficiency of the algorithm. The establishment of this hierarchical model clarifies the security level required by different users' privacy information in the e-commerce platform, and facilitates subsequent work such as selecting different encryption algorithms for different levels of privacy information and deciding the priority of calling resources.

After the processing of big data technology, the value of personal privacy has been further amplified. Driven by interests, many enterprises and illegal organizations have begun to collect, analyze, process, and resell user privacy information without restrictions. The flow of user privacy data within or between enterprises further increases the risk of data leakage. According to the Survey Report on the Leakage of App Personal Information released by the China Consumers Association in 2018, 85.2% of the respondents said they had encountered the problem of personal information leakage. The security situation of user privacy information is severe. While improving user privacy

regulations, it is also important to improve network service systems and strengthen privacy information encryption protection.

At present, solutions for protecting user privacy on e-commerce platforms mainly fall into two categories: one is to improve user privacy protection protocols, and the other is to improve information encryption technology. Exploring privacy protection from a rule-based perspective is not within the scope of this article, but in comparison, protecting user privacy through technical means is undoubtedly the most effective protection method for externally initiated privacy information theft activities.

This article proposes a layered encryption model PABB based on the importance of protecting personal information security under big data. From top to bottom, the security level is divided into user payment layer, user account information layer, user behavior information layer, and user basic information layer. It clarifies the security level required for different user privacy information, making it convenient to choose different encryption algorithms for different levels of privacy information in the future Determine the priority of resource calls and other subsequent work.

2. Layered Encryption Model

Based on the importance of protecting personal information security under big data, this article proposes a layered encryption model PABB for personal information recorded/stored on e-commerce platforms.

User payment/sensitivity/identity layer, including user ID number, account balance, bank card password, payment password and other sensitive information related to user property security. This article considers using the RSA algorithm with high security and low efficiency to encrypt the information in this layer.

User account information layer includes personal privacy information such as user account passwords, secure mobile phones, and secure email addresses. This information is related to the security of the user's account, and this article adopts the AES encryption algorithm with high security and efficiency.

User behavior information layer includes privacy information such as user consumption records, purchase records, search records, account consultation records, and account friends. This article selects the 3DES algorithm, a more secure encryption algorithm than traditional DES, to encrypt the information in this layer.

User basic information layer includes information such as user name, phone number, address, etc. The information on this layer will be partially displayed to the product seller, with the middle part replaced by "*".

In the process of conceptualizing the layered model, this article first developed a three-layer layered encryption model PAB, the Payment user payment/sensitive/identity layer; Account user account information layer, including account passwords, secure mobile phones, secure email, browsing records, purchase records, consumption records, search records, etc; Basic user basic information layer, including user name, phone number, address, etc. There is a significant difference in importance between behavior related information and account login related information in the Account layer. The information related to account login, such as account password, secure mobile phone, secure email, etc., is closely related to all information except payment in the account. Once the account login information is leaked, lower-level information will also be leaked. And these two parts of privacy belong to user uploaded data and user behavior records respectively, which do not comply with the definition of user personal privacy in e-commerce given in this article. Therefore, the Account layer is segmented into a new Behavior user behavior information layer.

In order to distinguish between the Account layer and the Behavior layer, the weight of the i-th element that reflects the security of the information layer is xi, and the value of the i-th element in the information layer is ai. The weight system W (x) is defined as equation (1):

$$W(x)=a_1x_1+a_2x_2+a_3x_3; \quad (1)$$

X1, the degree of association with user image, represents the degree to which user preferences and behavior patterns can be learned through this layer of information. This article sets the value of x1 to 2.

X2, the degree of correlation with user life, represents the degree to which information from this layer can affect users' lives outside of the platform. This article sets the x2 value as 4.

X3, which is related to account security, indicates whether the information in this layer can be used to log in to the user's account, and has a high weight. This article sets the x3 value to 5.

The user account information layer contains much less data than the user behavior information layer. It is true that information such as phone, email, and address can be used to simply infer user profiles, but the information contained is still too little and the error is too large. The leakage of information in the user account information layer will have a more significant impact on users' lives, and criminals will harass users through text messages, phone calls, and emails. The information in the user behavior information layer is mostly used for user group image analysis and market analysis, and leakage does not have a significant impact on user life. User account information is a necessary condition for logging in to a user's account on the platform, and account information is closely related to account security. Behavioral information is a record of the user's behavior after logging in to the account, and is not strongly related to account security.

Therefore, the values and weights of each layer are shown in Table 1, where $W_A(x)<W_B(x)$. Based on information security, the user account information layer requires a higher level of protection compared to the user behavior information layer.

Table 1. Statistical Table of A/B Layer Weight System

Layer	x1(2)	x2(4)	x3(5)	W
Account(A)	0.5	10	10	91
Behavior(B)	10	5	1	25

3. Algorithm Overview

3.1. RSA algorithm

The key generation process of the RSA algorithm is as follows: the system generates two large prime numbers p, q, calculates n=pq, and Euler functions φ (n) =(p-1) (q-1), randomly select one that satisfies gcd (e, φ (n) E=1 is used as the public key, while (e, n) is the encryption key, and the calculation satisfies ed=1 (mod φ (n) D is used as the private key, and (d, n) is the decryption key. Where p, q, φ (n) Confidentiality, n Public. The encryption process is shown in Figure 1.

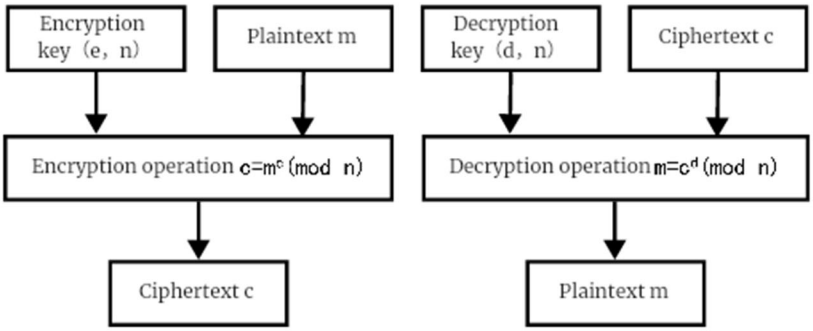

Figure 1. RSA Algorithm Encryption Process

3.2. AES algorithm

AES is a block cipher algorithm, which divides the plaintext into 128 bits each and encrypts a group of data each time until the entire plaintext is encrypted. AES algorithms are divided into three types based on the length of the key: 128 bits, 192 bits, or 256 bits. This article takes 128 bits as an example. Each round of AES algorithm encryption process includes four operations: byte substitution, row transformation, column transformation, and round key addition.

3.3. 3DES algorithm

DES is a fast encryption algorithm that operates on 64 bit data blocks using a 56 bit key. The encryption of each 64 bit plaintext block is generally divided into three steps: initial permutation, 16 rounds of cycling, and termination permutation. The encryption process is shown in Figure 2.

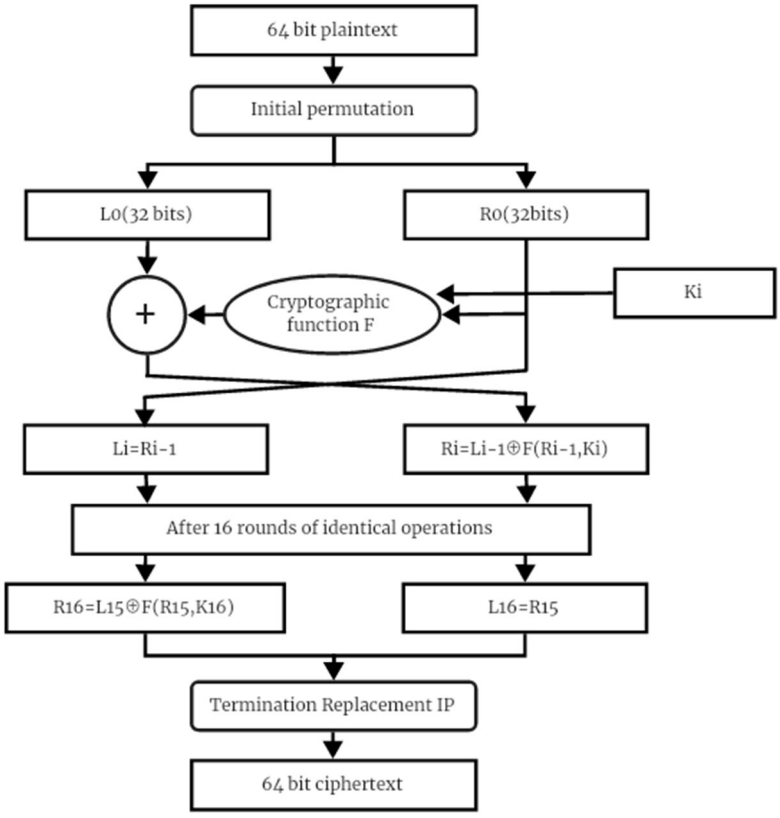

Figure 2. Data Encryption Standard encryption process

3DES, also known as Triple DES, is an improved version of DES. The algorithm encryption and decryption process is shown in Figure 3.

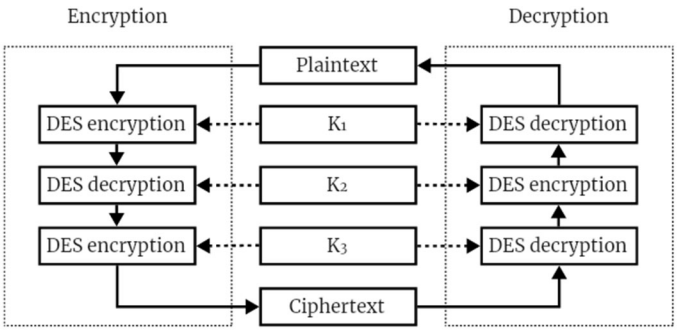

Figure 3. 3DES algorithm encryption and decryption process

4. Experiments

4.1. User Payment/Sensitive/Identity Layer

The fourth layer of user payment/sensitive/identity layer adopts RSA algorithm. It has performed 100 encryption operations on the fictitious bank card number (9082 1239 3192 3912), account amount (69082.23), and ID number (832184204206212851), and selected five representative data for visualization, recording their running time and average value as shown in Table 2. Using RSA algorithm for encryption and decryption takes longer on average and has lower efficiency. After encryption and decryption, the plaintext content can be restored intact.

Table 2. RSA Algorithm Encryption and Decryption Experiment Time/ms

Experiments	Bank card number	Account amount	ID number
	460	456	447
	405	504	455
	390	450	450
	398	479	479
	399	452	452
Average	411	468	457

4.2. User account information layer

The third layer of user account information layer adopts AES algorithm and performs 100 checks on a fictional phone number (16891211445) and email number, respectively (FictionalEmail@gmail.com) The encryption operation of account password (K4^dj&1e) was performed, and 5 representative data were selected for visualization. The running time and average value were recorded as shown in Table 3. The use of AES algorithm has high encryption and decryption efficiency, and after encryption and decryption, the plaintext content can be restored intact.

Table 3. AES algorithm encryption and decryption experiment time/ms

Experiments	Password	Phone number	Email number
	82	74	80
	97	82	78
	78	77	79
	77	76	75
	81	81	81
Average	83	78	79

4.3. User behavior information layer

In the second layer of user behavior information, the 3DES algorithm was used to perform 100 encryption operations on a fictional product name (New fashion T-shirt), consultation communication statement (I forget my password. What should I do next?), and friend's name (best friend Frank J), respectively, and their runtime and average values were recorded as shown in Table 4. The use of 3DES algorithm for encryption and decryption is relatively stable, with moderate efficiency. After encryption and decryption, the plaintext content can be restored intact.

Table 4. 3DES algorithm encryption and decryption experiment time/ms

Experiments	Product name	Communication	Friend's name
	366	374	367
	372	378	360
	372	373	374
	373	366	373
	373	373	368
Average	371	367	368

4.4. User Basic Information Layer

In the first layer of user basic information layer, the mobile phone number and name will be partially displayed to the product seller, and the middle part will be replaced with "*". This article conducted 10 hidden protections for user name (Amy Smith), mobile phone number (16810899272), and address (Second Floor, 40 White Horse street, London, L7 7AG, UK), and visualized a set of data. The calculation results are shown in Figure 4. The algorithm takes 1ms for the selected data. The replacement algorithm has high efficiency and can effectively hide important information.

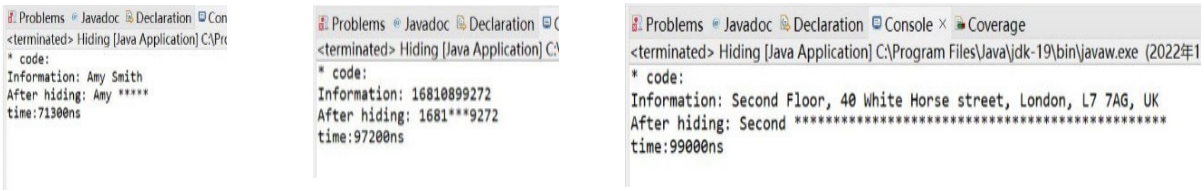

Figure 4. Calculation Results

4.5. Experimental Analysis

This article conducted 100 repeated experiments on each of the first three layers of data, randomly selecting and visualizing 5 sets of data. All three encryption algorithms were able to fully recover ciphertext, ensuring that the encryption and decryption process did not break the original data. By replacing, basic information can be effectively prevented from being exposed. In terms of algorithm efficiency, there is no pattern between the average time spent by each encryption algorithm and the length of the data string. The average encryption and decryption time using the RSA algorithm is 5x that of the AES algorithm and 1.4x that of the 3DES algorithm, which basically meets the efficiency requirements of the layered encryption model for the algorithms used in each layer.

5. Conclusion

Based on the importance of protecting personal information security under big data, this article proposes a layered encryption model PABB for personal information recorded/stored on commercial platforms, which can better help e-commerce platforms distinguish the security levels of different user information and choose more targeted encryption algorithms to protect user privacy. This article roughly selects RSA, AES, 3DES, and "*" replacement methods to protect privacy information at different levels, but there are still many aspects that need to be improved in the future, such as selecting more efficient or secure encryption algorithms, including ECC, EM2, etc; Provide a more detailed explanation and classification of the importance of privacy information at different levels; Simulate encryption and decryption of randomly generated data.

References

[1] CRAIN, M. (2021). A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE. University of Minnesota Press, Twin cities, Minnesota.

[2] OECD. (1999) The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda. OECD Publishing, Paris.

[3] Meng Wei (2007). Research on the Concept of E-commerce. Consumer Guide (02), 120-121

[4] Reng Ran (2003) Overview of the Concept and Characteristics of E-commerce. Modern Communication (01), 16-18

[5] Liu Yahui, Zhang Tieying, Jin Xiaolong, and Cheng Xueqi (2015). Personal Privacy Protection in the Era of Big Data. Computer Research and Development (01), 229-247