Hierarchical Model of E-commerce Privacy Protection Based on PPI Model

Zihao Lin(✉)

School of Information Engineering, Hangzhou Dianzi University, Hangzhou, China
rara07072022@163.com

Abstract. With the rapid development of Internet technology, people pay more attention to the protection of personal privacy in the big data platform to avoid the risk of data leakage while enjoying the Internet. Companies used encrypt databases or traditional inefficient encryption algorithms to protect privacy under the Internet, which leads to waste of resources and decline of security coefficient. The PPI model proposed in this paper splits data into different layers, and uses different encryption algorithms to protect data at different security levels. Experiments show that the PPI model largely avoids the loss of time and resources, and greatly improves the security of data protection.

Keywords: Privacy Protection · Data Encryption · Data Analysis · E-commerce

1 Introduction

With the gradual development of Internet, the privacy of users in e-commerce has always been concerned [1].

As shown in Fig. 1, user privacy has been stolen and embezzled frequently. In June 2018, Executes big data company leaked 2TB of privacy information by mistake, which led to the disclosure of 230 million people's privacy. In the same month, 1 billion pieces of express information of Yuantong were also leaked. After the information was reprocessed, the stolen information was packaged and sold at the price of 1 Bitcoin. In August of the same year, companies listed on the NEEQ involved in stealing 3 billion pieces of personal information, involving Baidu, Tencent, Alibaba and other 96 Internet companies nationwide. In September, Veeam, a Swiss data management company, leaked 445 million user data. In December 2018, Facebook's data leakage attracted worldwide attention. Its company leaked tens of millions of user data, including its private photos and other personal privacy. Later, the company was fined more than 1.6 billion dollars. As shown in Table 1,it shows the Data Privacy Disclosure Events and Consequences.

In order to better protect privacy, researcher pay more attention on cryptography. At the beginning of the typical password stage, people encrypts information with many classical password systems, such as Caesar password, Polybius password and Virginia password. Later, with the development of mechanical technology, the rotary cipher machine was born, making great progress in the development of cryptography. In the modern cryptology stage from 1945 to 1975, due to the requirements of information storage and

V. Gaikar et al. (Eds.): ECIT 2023, AHE 18, pp. 4–12, 2023.
https://doi.org/10.2991/978-94-6463-210-1_2

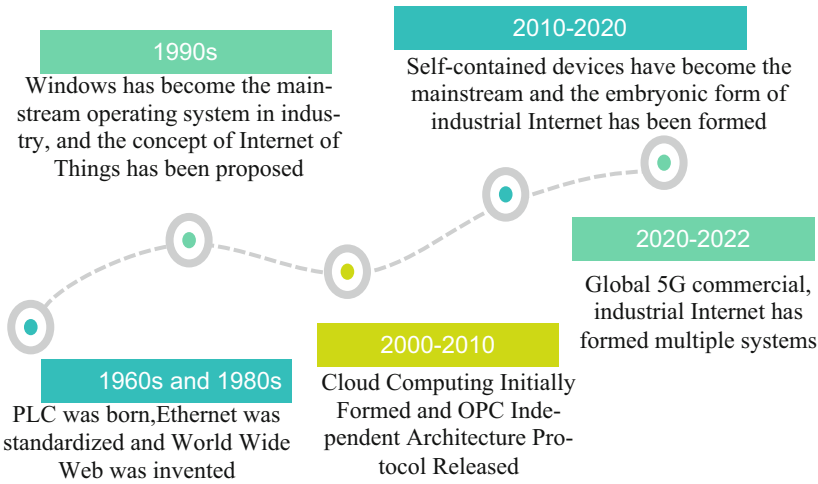

Fig. 1. Internet Development Trend(owner-draw)

Table 1. Data Privacy Leakage Incidents and Consequences(owner-draw)

Time Of Occurrence	Event Content	Causing Consequences
June 2018	Exatis big data company leaks 2TB of private information by mistake	About 340 million records are involved, the capacity is close to 2TB, covering 230 million people,and the privacy depth of these data is beyond imagination
	Yuantong 1 billion express information leakage	One billion pieces of information have been reprocessed, and the stolen information is packaged and sold in one bitcoin
August 2018	Companies listed on the NEEQ involve stealing 3 billion pieces of personal information	It is suspected of illegally stealing 3 billion pieces of user personal information, involving 96 Internet companies nationwide, including Baidu, Tencent, Alibaba, JD, etc.
September 2018	Swiss data management company Veeam leaked 445 million user data	The 445 million pieces of information include the name and residence of the victim, as well as organization size, IP address, etc.
December 2018	Facebook data leakage	The company was fined more than 1.6 billion dollars for divulging tens of millions of users' private photos and privacy

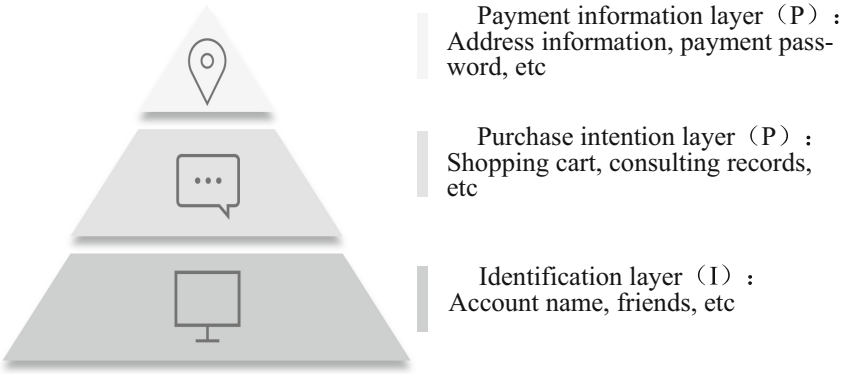

Fig. 2. Schematic Diagram of PPI Model Structure(owner-draw)

transmission in computer communication, cryptology has developed very fast for the consideration of information security. Now in the modern cryptography stage, W. Diffie and M.EHellman published a key consistency algorithm, namely DH algorithm, in 1976, marking that cryptography has entered the stage of public key cryptography.[2].

The PPI model proposed in this paper is a privacy encryption model based on e-commerce to protect the privacy information involved in the online payment process. In order to protect information of different security levels more effectively, this paper divides PPI model into three layers: identification layer, purchase intention layer and payment information layer (as shown in Fig. 2).

Among them, the identification layer contains the account name, fans and other information involved in the online payment process. This information is important to the user's shopping behavior, but does not involve the user's privacy. Therefore, dividing this information into user information layer and encrypting it with AES encryption algorithm can effectively protect user's personal information.

The purchase intention layer contains information such as the user's consulting record and browsing record, which involves the user's purchasing intention, so it has certain commercial value. However, this information does not directly concern the user's privacy, so dividing it into a buying intent layer and encrypting it with Blowfish encryption algorithm can effectively protect the user's purchasing intent information.

The payment information layer contains the user's address information, mobile phone number and bank card number, which directly relates to the user's personal privacy. Therefore, dividing the information into payment information layer and encrypting it using ECC asymmetric encryption algorithm with high security factor can effectively protect users' personal privacy information.

In this hierarchical way, the PPI model can use different encryption algorithms according to the security level of information, effectively protecting users' private information. In the online payment process, users' payment information, purchase intention information and personal privacy information are effectively protected.[3].

In summary, the PPI model proposed in this paper is a relatively more effective privacy encryption model, which can effectively protect users' privacy information in e-commerce. (see Table 2 for details).

Table 2. PPI Model Hierarchy Table(owner-draw)

Name Of Layers	Include Information	Encryption
Payment Information Layer	Address information, mobile phone, bank card number, payment password, and other information	AES
Purchase Intention Layer	Shopping cart, browsing records, evaluation records, search records and other information	Blowfish
Identification Layer	Account name, favorite stores, followers, fans, friends and other information	ECC

PPI model can not only protect users' privacy to a large extent in e-commerce and prevent data privacy from being infringed by lawbreakers, but also ensure the efficiency and security of the model. The contribution of PPI model proposed in this paper is as follows:

- This paper proposes a privacy encryption model based on e-commerce for the first time.
- Experiments are carried out to compare and analyze the performance of each secret algorithm and apply it to the privacy protection in e-commerce.
- This paper also selects the most suitable encryption algorithm after comparing various encryption algorithms and embeds it well in the PPI model.

2 Related Work

2.1 Symmetric Encryption Algorithm

DES encryption algorithm was developed by IBM in 1972, and is now widely used in many fields, such as MAC verification of financial transaction data packets, highway toll stations, etc., to protect the data therein [4]. In 1994, Blowfish encryption algorithm was gradually developed as a variable length key block encryption system, with encryption speed and security much higher than DES algorithm. In 1997, the National Institute of Standards and Technology of the United States issued the research and development plan for Advanced Encryption Standards (AES-FIPS), which determined a free and universal encryption algorithm to replace DES that can protect sensitive information. This algorithm solved the defect that 3DES algorithm could not be used for a long time due to the slow running speed of software, and has extremely high flexibility and feasibility.[5].

2.2 Asymmetric Encryption Algorithm

The RSA public key algorithm was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1978.[6] The algorithm is complex in operation, difficult to crack, but slow in speed. Elliptic encryption algorithm (ECC) was originally proposed by Koblitz and Miller in 1985. It uses the difficulty of discrete logarithm of Abel group formed by points of elliptic curve over finite field to realize encryption, decryption and digital signature

[7]. In 1991, the DSA encryption algorithm was proposed by the National Institute of Standards and Technology and adopted by the federal information processing standard in 1993 [8].

3 Method

The current encryption algorithms include symmetric encryption algorithms and asymmetric encryption algorithms. In symmetric encryption algorithms, there is only one key involved, and the sender and receiver jointly hold this key to encrypt and decrypt data. The common symmetric encryption algorithms are: DES, 3DES, AES and Blowfish. It can be seen that AES and Blowfish encryption algorithms are not only faster and more efficient, but also more secure than DES and 3DES (as shown in Table 3).

Asymmetric encryption algorithm is more secure but slower than symmetric encryption algorithm. The main asymmetric encryption algorithms are IDEA, RSA and ECC. Compared with RSA and DSA, ECC asymmetric encryption algorithm is less computational, faster to process, not only is it many times more resistant to attack under the same key length, but also takes up less storage space, ECC key size is smaller than RSA and DSA (as shown in Table 4) [9].

Based on the above comparison, three encryption algorithms, AES, Blowfish and ECC, are selected to encrypt for different security levels.

AES algorithm, also known as Rijindael encryption method, is a block encryption standard adopted by the United States federal government. It has been analyzed by many

Table 3. Symmetric Encryption Algorithm(owner-draw)

Symmetric Encryption	Implementation Method	Encryption Speed/Security	Resource Consumption
DES	Use 16 cycles, exclusive OR, replacement and shift operations	Slow/Low	The grouping is short, the key is too short, the password life cycle is short, and the operation speed is slow
3DES	Based on DES, a piece of data is encrypted three times with three different keys	Slow/High	Higher intensity and high resource consumption
AES	Based on permutation and permutation	Fast/High	Faster data encryption method, compatible with different products, and fast
Blowfish	Generate Blowfish sub key, and conduct 16 iterations to obtain output data	Fast/High	With military level security performance, the computing speed is far lower than that of traditional AES and DES

Table 4. Asymmetric encryption algorithm(owner-draw)

Asymmetric Encryption	Implementation Method	Encryption Speed/Security	Characteristic
RSA	Based on large number decomposition	Slow/Factorization Dependent on Large Numbers	Public key algorithm that supports variable length keys, and the length of file blocks to be encrypted is also variable
ECC	Elliptic Curve Cryptography	Fast/High	Strong resistance to attack, small amount of computation, and fast processing speed
DSA	Discrete Logarithm Problem Based on Integer Finite Field	Fast/Similar to RSA	

parties and is widely used in the world. The AES algorithm first expands the key to 40 new columns, gets 10 sets of wheel keys by XOR, then replaces each element in the plain text grouping by S-box, then replaces the row and column, and finally adds the round keys, and replaces the result by XOR operation in the column by column with the plain text grouping matrix. Then the ciphertext is finally obtained by repeating the cycle of subprocesses (e.g., AES-128 normally cycles this process 10 times, AES-192 normally cycles 12 times).

ECC encryption algorithm is a public key encryption algorithm, which can be used with a shorter key to achieve a high degree of security, and has been gradually applied. The ECC algorithm first lets Party A select an elliptic curve Ep (a, b) and a point on the curve as the base point G, then selects a large number k as the private key, and generates a public key Q = kP, then sends Ep (a, b) and k, G to Party B. Party B receives and encodes the plain text to a point M on Ep(a, b), generates a random number r, then calculates the point C = (rP, M + rQ) and sends it to Party A. Party A then obtains M through M + rQ-k(rP) = M + r(kP)-k(rp), and finally decodes M to get the plain text.[10].

Blowfish algorithm is a symmetric group encryption algorithm proposed in 1993. It encrypts one bit group at a time, uses variable length keys for internal encryption. The encryption process first preprocesses the keys, then encrypts the information. It is fast, safe and simple [11].

In this paper, AES and Blowfish, the symmetric encryption algorithms with lower security level and faster speed, are respectively applied to the first two levels of PPI model: identification layer and purchase intention layer; Then, the asymmetric encryption algorithm ECC is applied to the payment information layer, which is the third layer with the highest security requirements.

4 Experiment

The system used in this experiment is Windows 10, the processor model is Intel (R) Core (TM) i7-10875H CPU @ 2.30 GHz, and the Java version used is 1.8.0_ 201, using the software IntelliJ IDEA 2019.3.3.

This experiment conducted a simulation test on the text content at different levels of the PPI model. The first layer of the PPI model is the identification layer, so the content of the simulation text is "Testname", and then input it into the AES model to get the ciphertext as shown in the table, and then decrypt the ciphertext with AES; Similarly, the second layer is the purchase intention layer, so the simulation text "good book, good quality" is substituted into the Blowfish model, and then the third layer is the payment information layer. The simulation data is Hangzhou, Zhejiang Province, which is also brought into the model ECC, and the results are shown in the Table 5.

As shown in Table 6, the AES encryption time is 1339.0 ms, 1331.0 ms and 1326.0 ms respectively, the average encryption time is 1332.0 ms, and the average decryption time is 2397.3 ms. The average encryption time of the data information of the second

Table 5. Text Information Simulation(owner-draw)

Encryption Algorithm	Before Encryption	After Encryption	After Decryption
AES	Testname	c47TEZ+YHUGCJW3UW1GXMQ==	Testname
Blowfish	Good book, good quality	57537c3caa6b00e0a27b9e60c3a054fb 01863a73a83a740865e3bb961626d0ce 2df1faacc46e405281c377be979a24816f279406278ebaa8	Good book, good quality
ECC	Hangzhou, Zhejiang Province		Hangzhou, Zhejiang Province

Table 6. Table of Experimental Values(owner-draw)

Encryption Algorithm	Encryption Time	Average Encryption Time	Decryption Time	Average Decryption Time
AES	1339.0 ms	1332.0 ms	2278.0 ms	2397.3 ms
	1331.0 ms		2428.0 ms	
	1326.0 ms		2486.0 ms	
Blowfish	68.0 ms	64.0 ms	55.0 ms	57.0 ms
	61.0 ms		67.0 ms	
	63.0 ms		49.0 ms	
ECC	1253.0 ms	1169.0 ms	1755.0 ms	1892.3 ms
	1128.0 ms		2089.0 ms	
	1126.0 ms		1833.0 ms	

security level by Blowfish is about 20 times lower than that of the AES encryption algorithm, and the average decryption time is also 45 times lower, 64.0 ms and 57.0 ms respectively. The data encryption time of the highest security level by ECC is 1169.0 ms, and the decryption time is 1892.3 ms, It is close to the time required by the AES algorithm, but also far higher than the Blowfish algorithm. It can be seen that this is a protection strategy of exchanging time for security, making the overall PPI model more secure and stable.

5 Conclusion

With the rapid development of the Internet, more and more people attach great importance to data privacy protection. The PPI model proposed in this paper has solved the problem that the waste of data encryption resources and time has led to the reduction of efficiency. A new idea has been proposed for this new challenge. For the first time, a privacy protection model PPI under e-commerce has been proposed, which layers the data security levels, and uses different encryption algorithms to protect the data privacy of different security levels, The experimental results show that the PPI model gradually increases the security level from bottom to top, and encrypts and protects data at different security levels by means of exchanging efficiency for security. To sum up, the experiment proves that the model is effective for privacy protection and reduces the loss of time and resources.

References

1. Feng Dengguo, Zhang Min, Li Hao.Big Data Security and Privacy Protection[j].Chinese Journal of Computers,2014,37(01):250–262
2. Ding Yuncong, Li Xi, Wang Yulu.A review of cryptography[j].SICHUAN CEMENT,2017(03):372
3. Bai Lanhua.Research on Database Encryption Method[d].Sichuan:University of Electronic Science and Technology of China,2020(08)
4. Zhang Jie,Zhu Lijuan.Analysis and Implementation of DES Encryption Algorithm[j].SOFTWARE GUIDE,2007(03):95–97
5. Zhang Yuanjin.Analysis of 3DES packet encryption algorithm model[j].Computer and Digital Engineering,2014(08):164–167
6. Wang Jin.Research on RSA encryption algorithm[d].Liaoning:Shenyang University of Technology,2006(10)
7. Qin Zhiguang.Research on the current situation and development of cryptographic algorithms[j].Journal of Computer Applications,2004,24(02):3–6
8. Meng Yanhong, Qin Weijia, Lv Haihua.Research and Comparison of Two Cryptosystem Encryption Technologies[j].Journal of Shenyang University of Technology,2003,25(05):72–74
9. Yang Wei.Data Encryption and Information Security[d].Hefei:Hefei University of Technology,2007(03)
10. Li Wenfeng, Du Yanhui.Application of cryptography in network security[j].NETINFO SECURITY,2009(04):44–46
11. Zhong Qianchuan, Zhu Qingxin.Analysis of Blowfish Cryptosystem[j].Journal of Computer Applications,2007,27(12):62–63