The Application and Exploration of Database in Law

- Reasonable Preservation and Protection of Consumer Information in Online Transactions

Yusheng Zhao[1,a], Zhaoqing Wang[2,b], Guorong Zhong[1,*]

[1]International School, Beijing University of Posts and Telecommunications Beijing, China

[2]School of Information& Communication Engineering, Beijing Information Science& Technology University, Beijing, China

*Corresponding author email: 2016213302@bupt.edu.cn

[a]zhaoyusheng@bupt.edu.cn;[b]mj741561@163.com

Keywords: Database, PPSDS, DPSASA, Reasonable preservation of consumer information, Protection of consumer information.

Abstract: In the era of big data, the application of the database is very extensive, and the implementation of many laws is inseparable from the application of the database [1]. According to General Principles of the Civil Law of the People's Republic of China and Consumer Protection Law of the People's Republic of China, this paper finds the loss of consumer information in the current online transactions. In order to study the feasibility of the legal provisions, this paper applies the PPSDS (Privacy Protection in Secure Database Service) database model and the DPSASA (the Database Protection System Against SQL Attacks) database model [2][3]. The former realizes the reasonable preservation of information by decomposing the original database. The latter achieves the defense against SQL attacks by filtering the violation characters in the request, thereby achieving the purpose of protecting the information. At the same time, this paper draws on the advantages of EU law and related policies, and combines the above two models to propose an optimization plan to protect consumer information in online transactions.

1. Introduction

In electronic transactions in the era of big data, databases that store consumer information are often attacked. Although there are laws such as civil law and consumer rights protection law to protect consumer information rights, in fact, due to the short time and rapid development of electronic trading exhibitions, there are still many problems in implementing these laws [3].

In online transactions, there are a variety of ways to obtain consumer information, but this paper mainly focuses on the problem of the attacker illegally obtaining consumer information. In this paper, the database is decomposed according to the quasi-identifier by applying the PPSDS database model. And the PPSDS database model also implements the front-end data decomposition, query processing and other functions, thus achieving the purpose of reasonable preservation of consumer information. At the same time, this paper applies the DPSASA database model to separate the front end from the back end. And it can filter the client's request to prevent possible SQL attacks, thus protecting consumer information. Finally, this paper draws on EU law and related policies, and combines the above two technologies to optimize the method of protecting consumer information in online transactions.

The second part of this paper will introduce the background of China's information protection for consumers in online transactions, and the third part will combine the advantages of the EU and the two database models of PPSDS and DPSASA to propose a new way to protect consumer information. Program. The fourth part of this paper will summarize the full text.

  DOI: 10.25236/mfssr.2019.101

2. Background

2.1 Legal support for consumer information protection in online transactions

a) General Principles of the Civil Law of the People's Republic of China

Article 128

Where the law has special provisions on the protection of civil rights of minors, the elderly, the disabled, women, consumers, etc., it shall be in accordance with its provisions.

b) Consumer Protection Law of the People's Republic of China

Article 29

Operators shall, in the collection and use of consumer personal information, follow the principles of lawfulness, rationality and necessity, and clearly indicate the purpose, manner and scope of the collection and use of information, with the consent of the consumers. Operators shall disclose and use the personal information of consumers, and shall disclose their rules for collection and use, and shall not violate the provisions of laws and regulations and the collection and use of information by both parties.

The personal information collected by the operator and its staff must be kept strictly confidential and must not be disclosed, sold or illegally provided to others. Operators should take technical measures and other necessary measures to ensure information security and prevent consumers from leaking or losing personal information. Remedial measures should be taken immediately in the event of information leakage or loss of information.

2.2 Loss of consumer information

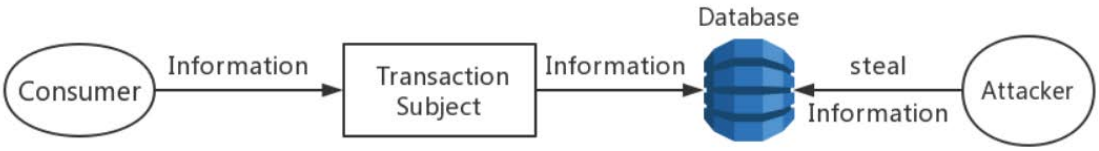

Figure1. Loss of consumer information

2.3 Reasonable preservation of consumer information

According to the provisions of the Chinese Consumer Protection Law, the subject of online transactions is obliged to properly preserve consumer information. However, many databases currently have a single storage format. Once attacked by an attacker, all the information of the consumer will be completely leaked, causing extremely serious consequences[2]. Therefore, how to ensure the rationality of consumer information storage will become a core issue.

2.4 Protection of consumer information

According to the provisions of the Chinese Consumer Protection Law, the subject of online transactions is obliged to prevent consumers from stealing information. Web services typically use a database to store information, and almost all sites should use the database. Many attacks are against the database, the most common is the SQL attack. At present, many databases lack an effective protection mechanism in the front stage, which is easy for an attacker to invade and obtain important information in the database. Therefore, it is necessary to establish an effective consumer information protection mechanism for SQL attacks [3].

2.5 Feasibility of Chinese law

According to the General Principles of the Civil Law of the People's Republic of China Article 128, which clearly emphasizes the protection of consumer rights, this is very reasonable.

According to the Consumer Protection Law of the People's Republic of China Article 29, it imposes clear restrictions and requirements on the behavior of online transaction subject to collect and store consumer information. It includes the need to obtain consumer consent for the collection of information, strict confidentiality of consumer information, and the necessary measures to protect consumer information. Therefore, it is feasible to use various database models to protect consumer information, and the restrictions on the transaction subject are also reasonable.

According to the Criminal Law of the People's Republic Article 253 [Infringement of Citizens' Personal Information], it clarifies the consequences of illegally obtaining consumer personal information. Besides, it has a deterrent effect on some potential criminals and indirectly guarantees the safety of consumer information. This law is feasible and reasonable.

3. Optimize the optimization of consumer information in online transactions

3.1 Optimization of methods for saving and protecting consumer information

3.1.1 Reasonable preservation of consumer information

In view of the problems in Section 2.3, this paper adopts the PPSDS database model to optimize the storage method of consumer information, as shown in the Figure 2. The general architecture of a distributed secure database service consists of a trusted database management system front end and two or more servers that provide database services [2].

The server provides reliable content storage and data management to protect privacy. The trusted front end provides three functions:

1) Data decomposition. The trusted front end divides the unencrypted data into different database systems by automatically detecting the quasi-identifiers according to different attribute values, and stores the schema metadata of the relationship decomposition in the trusted front end. The quasi-signifier here is a combination of multiple elements of the source database, and this combination can achieve a high degree of discrimination in the original data set.

2) Query processing. The query received by the trusted front end needs to be converted to the appropriate SQL subquery sent to the server, and the results need to be collected and post processed before being returned to the user application in the appropriate form.

3) Metadata repository. The metadata repository of the trusted front end stores the schema metadata of the relationship decomposition, the generalization involved in the probabilistic anonymization, and the statistical information of the query optimization. All data in the metadata repository can be used to implement efficient database queries.

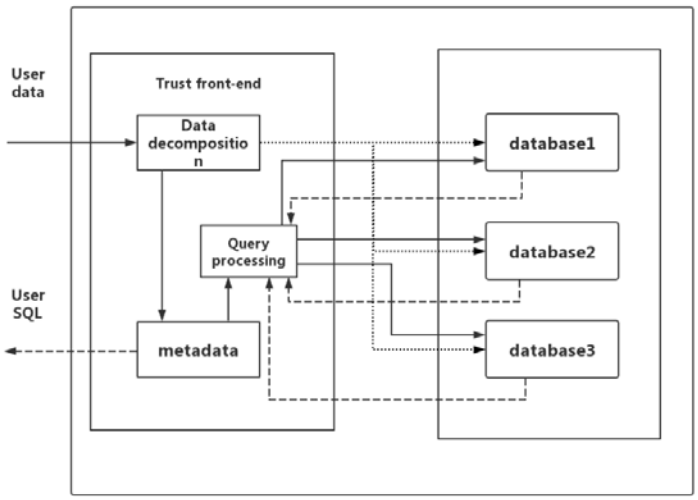

Figure 2.The System Architecture

At the same time, the model will automatically decompose the original database into two or more small databases according to the original database, using the automatic detection method of quasi-identifiers and the relationship decomposition method based on quasi-identifiers.

Subsequently, through the application of the front-end query processing function, the original SQL statement is properly converted to ensure the normal operation of the query. Since this model only stores part of the consumer information in one database, the significance of the attacker stealing a database information is greatly reduced. Therefore, this model realizes the reasonable preservation of consumer information by decentralizing the database.

3.1.2 Protection of consumer information

In view of the situation encountered in Section 2.4, this paper applies the DPSASA database model, mainly to protect the dynamically constructed SQL scenario and prevent unauthorized users from doing some damage to the database[3]. As the Figure 3 shows.

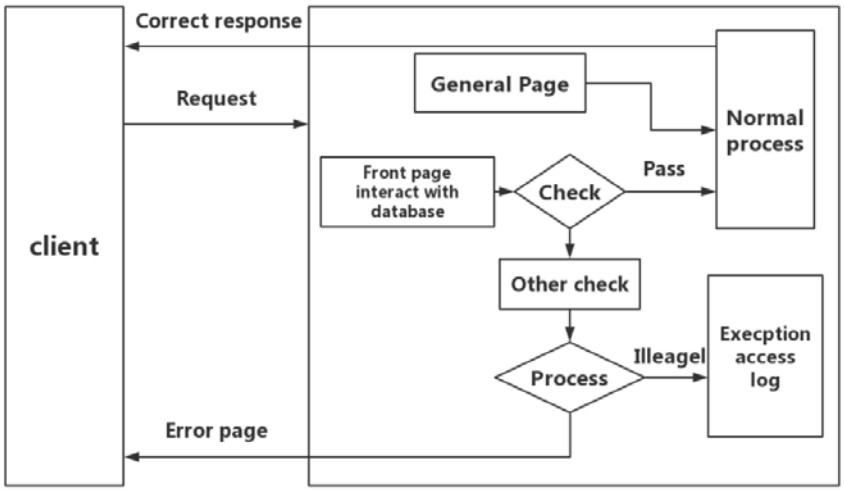

Figure 3.The Protection Model

The server distinguishes the request from the client. If the request is a static page, it goes to the normal process of the normal page; if the request requires the home page to interact with the database, the corresponding SQL statement is checked. If the SQL statement passes the check, it goes to the normal process, otherwise it performs error handling.

The main method:

1) Filter illegal characters to prevent attackers from modifying the meaning of SQL commands. If you don't check it, there will be some damage. For example, a query page : findproduct.asp?Id = 1, the original design intention of the programmer is to display the data Id as 1, if the attacker constructs the following statement : findProduct.asp?Id = 1; delete the Table management, it can be simple Delete database Table management [5]. Therefore, filtering illegal characters is mainly for this situation. Table 1 lists the potentially dangerous characters. In the query statement, any occurrence of such a character will not pass the check and enter the exception handler [3].

Table 1. Illegal Characters[3]

Query delimiter	String delimiter	Comment delimiter	The beginning of extended stored procedures
;	‘, ’	/* , */	Xp_

2) Restrict user permissions. This model makes it impossible for users without corresponding permissions to implement SQL statements.

3) Check the number of records returned by the query. If it does not match the expected result, the query fails to prevent large batches from stealing data.

This model achieves the purpose of blocking the attacker's SQL command by screening the input SQL command, thus achieving the purpose of protecting the consumer information.

3.2 EU's advantages in protecting consumer information

Table2. The Advantages of EU

Category:	Name:	Advantages:
Law	Data Protection Directive	Uniform requirements for the protection of personal data of its member states
Law	Directive 2002/58 on Privacy and Electronic Communications	Special specifications for personal information processing and privacy protection in the field of electronic communications
EU Department	EU Data Protection Working Group	Responsible for investigating the application of private data by enterprises
EU position	European Data Protection Supervisor	Ensure that all EU institutions and organizations respect citizens' privacy when dealing with citizen personal data
EU member states	Individual Personal Information Protection Act	Adapt to the specific situation in the country

Due to the special cooperation between EU countries, it is very important to ensure the confidentiality of information between countries' trade. All member states of the European Union have established their own set of personal information protection laws within the scope of the unified guiding law to adapt to their specific conditions. At the same time, the EU data protection group has been set up within the EU to conduct repeated investigations on the application of private data for most companies. In addition, the European Union has set up the European Data Protection Supervisor to supervise and guide the confidentiality of personal information of companies in various countries.

3.3 Optimization results in combination with EU advantages

The problem with Chinese law is that it is too general and not practical. The EU has a relatively complete mechanism in this respect. China's provinces can learn from the practices of EU member states and, within the scope of the Consumer Protection Law of the People's Republic of China Article 29, develop a consumer information protection law that is adapted to the province's situation. This also satisfies China's regional autonomy system. At the same time, China can also follow the EU's consumer information protection team and consumer information protection commissioner to supervise and guide the use of consumer information in domestic enterprises. Therefore, the awareness of domestic enterprises on the protection of consumer information in online transactions can be greatly improved, and the two database models proposed in this paper can be applied to finally realize the reasonable preservation and protection of consumer information in online transactions.

4. Conclusion

This paper applies the database to the direction of consumer information rights in online transactions in China's current laws. After discovering that there are many problems that the transaction subject does not pay attention to consumer information protection and the existence of an attacker illegally obtaining consumer information. This paper combines Chinese law and proposes a solution to the problem of PPSDS database model and DPSASA database model. The PPSDS database model mainly solves the problem of reasonable preservation of consumer information in online transactions, while the DPSASA database model solves the problem of protection of consumer information in online transactions. Finally, this paper combines the

advantages of EU law and related policies, and proposes an optimization plan to protect consumer information in online transactions.

References

[1] Elmasri, R., & Navathe, S. B. (2011). Database systems (Vol. 9). Boston, MA: Pearson Education.

[2] Yonghong, Y. (2010, April). Privacy protection in secure database service. In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (Vol. 1, pp. 218-222). IEEE.

[3] Yan, Y., Zhengyuan, S., & Zucheng, D. (2011, March). The database protection system against SQL attacks. In 2011 3rd international conference on computer research and development (Vol. 3, pp. 99-102). IEEE.

[4] Zhang Wei. On consumer privacy and legal protection in online transactions [J]. Law and Economy, 2019 (01): 87-88.

[5] Date, C. J., & Darwen, H. (1987). A Guide to the SQL Standard (Vol. 3). New York: Addison-Wesley.