International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 35-42
http://dx.doi.org/10.14257/ijsia.2015.9.6.04

Design of Distributed Pharmaceutical Retail Management System Based on Advanced Encryption Standard Algorithm

Jingjing Yang, Yuanqiang Wang and Xiao Zhang*

School of Information Science and Engineering, Hebei North University, Zhangjiakou, Hebei, China
*r78z-yang@126.com,*yjr78z@gmail.com*

Abstract

To meet the demand of digitizing progress of pharmaceutical retail industry, there are various kinds of software are made for pharmaceutical retail enterprise. However, much commercial software on the market fails to meet the demand of data transmission safety. Therefore, a novel system was designed for medium size pharmaceutical retail enterprise with multiple branches. It is designed to digitize the process of retail operations including management of stock, order client, staff, product, branch and warehouse. Advanced Encryption Standard (AES) algorithm was used to secure the data transmission on the Internet. The system can be deployed[1] in pharmaceutical retailing, hospital prescriptions issues, pharmaceutical company management, medical supplies market, medical devices market and hospital staff management. With minor modification the system can be deployed to other retail or wholesale industry.

Keywords: *Retail Management; Database; AES Algorithm; Encryption; Authentication*

1. Introduction

Marketing management, a business discipline which centers on the practical application of marketing strategies and the management of an corporation's marketing resources and behaviors. Globalization has made the corporations to market beyond the boundaries of their own nations, leading international marketing extremely important and an integral part of a corporation's marketing strategies [1]. Marketing managers are often responsible for influencing the opportunities and composition of customer demand accepted definition of the term. To a certain extent, it is on account of the role of a marketing manager can vary important on the basis of a business. For example, in a large corporation, the marketing manager may act as the overall general manager of his or her assigned product [2]. To create an effective, cost-efficient marketing management strategy, firms must possess a detailed, objective understanding of their own business and the market in which they operate [3]. The discipline of marketing management often overlaps with the related disciplines of planning in order to analyse these issues.

Pharmaceutical marketing is the business of advertising or otherwise promoting the sale of pharmaceuticals or drugs. To simplify the concept, we call pharmaceutical marketing as the pharmaceutical sales. In many countries, the spending of the sales of the pharmaceutical are much higher than the pharmaceutical researches [4-5]. Take Canada as an example, $1.7 billion was spent in 2004 to market drugs to physicians; while in the United States, $21 billion was spent in 2002 [6]. In 2005, money spent on pharmaceutical marketing in the US was estimated at $29.9 billion with one estimate as high as $57 billion [7]. When the US numbers are damaged, there was 56% free samples and 25% pharmaceutical sales representative "detailing" (promoting drugs directly to) physicians. In addition, 12.5% was direct to user advertising, whereas 4% on other spending in

*Corresponding Author

ISSN: 1738-9976 IJSIA

hospitals, and 2% on advertisements [6]. In Landefeld's opinion [7], evidences show that marketing practices can negatively affect both the health care profession and patients. On the basis of this reason, we paid our attentions to develop a handy pharmaceutical sales management software using relevant algorithm.

According to the software field, there are some relevant software offering the services of pharmaceutical marketing. However, most of them are considered to be the attachment of the sales software, which are not easy to handle for users. Therefore, we formulated our targets to be easy operate and good user experience.

2. Design Diagram of Distributed Pharmaceutical Selling Management System

The design of the Distributed Pharmaceutical Selling Management System is shown as follows:

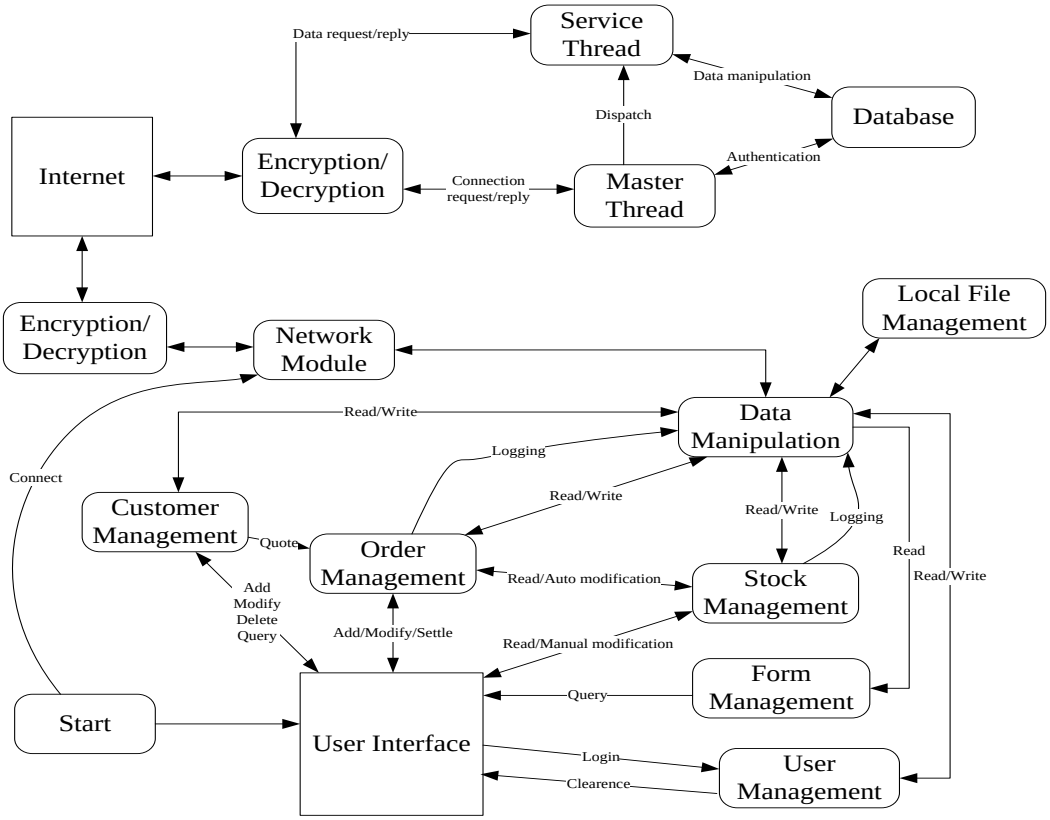

Figure 1. Design Diagram of Distributed Pharmaceutical Selling Management System

Figure 1 shows a description of the internal interactions between modules of the system. In client program, each management module is connected with user interface and the data manipulation module, which manipulates data in both remote server database and local file system. Every time when records of orders or stock are changed, a log will be automatically generated and written into local file system. With both remote and local data source, each client of this system could run properly under circumstances of network failure or server failure. Obviously it is possible that the data in local file and in remote database are different. To restore from such situation, the system need to synchronize the data between local file and remote database every time the server-client connection is established.

On server side, the master thread is designed to verify and accept client connection request, and then dispatch the client to a service thread for data transmission after creating one. The service thread is in a constant loop that receive data request from client, send the data request to database, and finally send back the result of requests.

Between server and clients, data of this system goes through the internet. Therefore approaches of encryption and decryption are needed to ensure the safety of sensitive commercial data. In this case, AES [8-11] algorithm is used in the encryption and decryption module.

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on the Rijndael cipher [12] which is a family of ciphers with different key and block sizes. For AES, three members of the Rijndael family are selected, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

3. Description of AES

There are four main stages for AES algorithm, key expansion, initial round, rounds and final round.

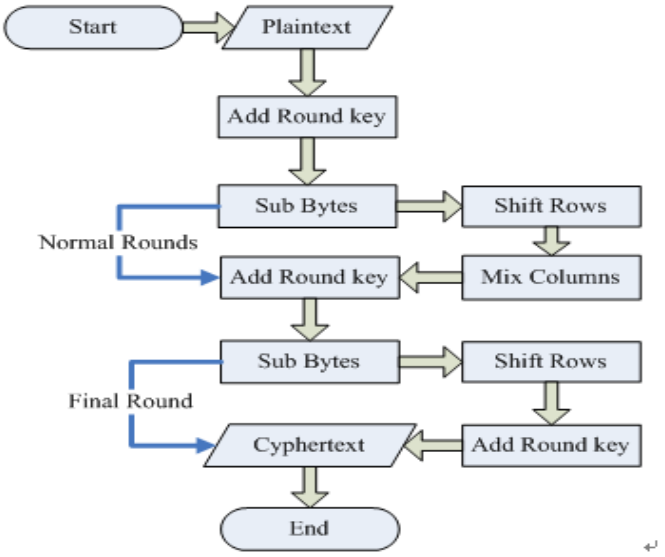

Figure 2. Flow Diagram of AES

Here, we present the descriptions and explanations of Figure 2, which are shown as follows:

Add Round Key: each byte of the state is combined with a block of the round key using bitwise exclusive or.

Sub Bytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

Mix Columns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

As it is considered save, AES is widely used in various systems containing sensitive data such as bank system and military systems. Therefore we can trust the data going through the Internet to be save under encryption of AES.

Using the AES algorithm shown in Figure 2 above, we can achieve the great assumption of developing the system for the distributed pharmaceutical retail management.

4. Core Code of the System

Here, we present the original encryption of the software of pharmaceutical retail management system we developed. One should note that the code shown by Figure 3 is the core code, due to the limitation of the article length, rather than the completed code set of the system in our research. However, every well-trained scientists and technicians of the field of computer science or software engineering can extract the useful parts of the core code shown by Figure 3 below and repeat the system presented by this article. For inducing more discussions with readers and our further studies, we decided to public this core code without any reservation and we hope that it will be useful for other relevant researches. However, we do not hope that the core code of our system will be used in any commercial use without the permissions of all of the authors in this paper.

In the style of C++, the encryption code in this system is shown in Figure 3 below based on open source library OpenSSL [13].

```
int encrypt128( char* in_buf, char* out_buf, int size, unsigned char* ckey )
{
	unsigned char* buffer =(unsigned char*) in_buf;
	unsigned char* iv = new unsigned char[32];

	if (size > 200 * 1024 * 1024){
		cout<<"Input is too large"<<endl<<"Halting..";
		return 0;
	}

	//padding
	int padding_size = 16 - size % 16;
	char padding_content = padding_size;

	for (int i = 0 ; i<padding_size ; i++){
		buffer[size+i] = padding_content;
	}

	cout<<"Encrypting..."<<endl;

	//encryption
	int block_num =size / 16 +1;
	AES_KEY key;
	AES_set_encrypt_key(ckey, 128, &key);

	memset(iv,0,32);
	for (int i = 0; i<block_num;i++){
		AES_cbc_encrypt(buffer+i*16,buffer+i*16,16,&key,iv,AES_ENCRYPT);
	}
	buffer[block_num*16] = 0;

	cout<<"Encryption complete"<<endl;

	return block_num*16;
}
```

Figure 3. Core Code of the System

Figure 3 presents the core code of the system we developed. We have simplified the code we developed and obtain a time-saving system for computers, which is extremely adaptive to most of the micro-microcomputers.

5. User Interface

Before entering the main surface, users need to login with a username and a password. Here we present the surface of login we designed in Figure 4:

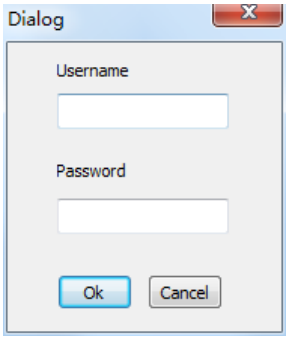

Figure 4. Login: Input Username and Password to Login

By clicking on different tabs to switch among Stock, Order, Client, Staff, Product, Branch and Warehouse management surface, we can obtain the data of corresponding tabs, which will be shown in the data area. In order to edit data of any tabs, we can choose a line of record and press the "add", "modify" or "delete" on the right part of the surface in the system.

The state bar in the bottom shows connection state between the server and the client, the current username and the clearance level of the user. Details of the main surface is presented in Figure 5:

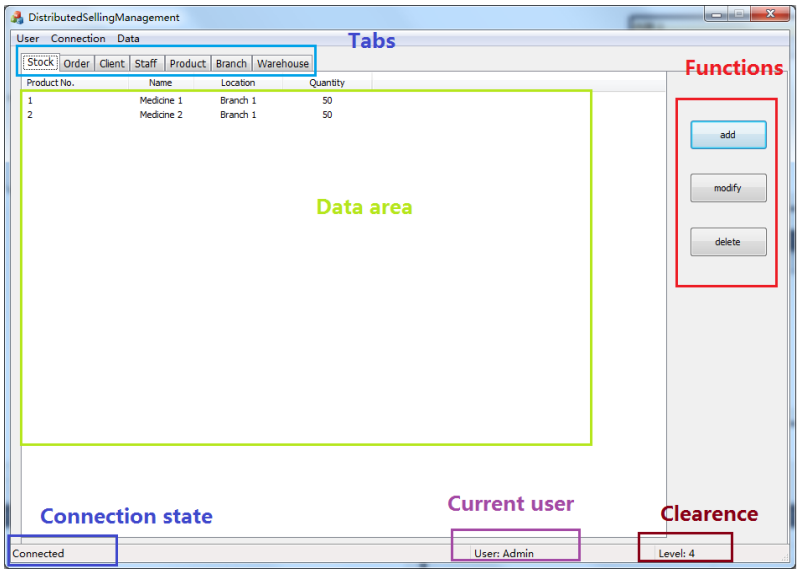

Figure 5. Main Surface of the System

Figure 5 shows the main surface of the distributed pharmaceutical retail management system, we can operate all the main functions of this system in this main surface.

The style of order detail dialog is similar to the main surface. After each modification, the total price of the order will be automatically modified and shown on the surface.

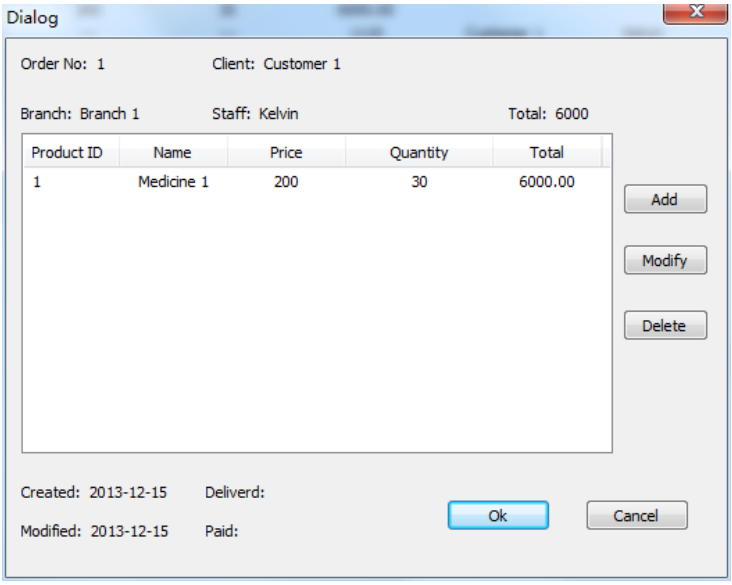

Figure 6. Surface of the Order Detail

Figure 6 shows the designed surface of the order detail. Users can make detailed orders in this operation surfaces. And at the same time, the details of the parameters in the system can be shown by this surface. It is designed for the convenience of users. Users can simply revise the parameter they want, adding different terms to adapt their works. The software's user-friendly feature can be shown in relevant operations. Users can only press the relevant buttons and then achieve their orders to the system.

6. Applications and Discussion

According to the tests and practical applications, the distributed pharmaceutical selling system is proved to be applicable and easy for users to operate. The application is extensive and confidential due to the formulation of the system. It can be used in the field of pharmaceutical sales, hospital prescriptions issued, pharmaceutical company management, medical supplies market, medical devices market and hospital staff management. Compared to the other existing pharmaceutical management software, distributed pharmaceutical selling system can be operated easily so that users have no need to be trained.

What is more importantly, our research on the distributed pharmaceutical selling system is not limited to the medical areas. The core code can also be modified and used in order to adapt various environments and applications. For example, it can also be used in super markets, college retails, community retails and export trades. It shows that the distributed pharmaceutical selling system is extremely flexible in practical applications [14-18].

Although the distributed pharmaceutical selling system has achieved a good user feedback, it's still necessary to be modified in order to develop a comprehensive and strong management system. When establishing the connection between server and client, it is better to use a public-key algorithm to exchange a session key used in AES data encryption.

7. Conclusion

Nowadays, there is a large number of software that are designed for pharmaceutical retail areas. However, among all these software, most of the commercial software on the market fails to meet the demand of data transmission safety, which would be a crucial problem in relevant fields and research.

Advanced Encryption Standard (AES) algorithm is a crucial algorithm that can be used for addressing the security problems in software engineering. Here, we use this important algorithm for a novel application of the retail system in order to ensure the effectiveness and security of the pharmaceutical retail system.

In this paper, we provide a novel distributed system for pharmaceutical retail system for medical related services. It is designed to digitize the process of retail operations including management of stock, order client, staff, product, branch and warehouse. AES algorithm was used for securing the data transmission on the Internet. The system can be deployed in pharmaceutical retailing, hospital prescriptions issues, pharmaceutical company management, medical supplies market, medical devices market and hospital staff management. With minor modification the system can be deployed to other retail or wholesale industry, showing that this system have an extremely high adaptability for practical applications. Also, we public the core code of this system we developed without any reservation in order to give more discussions with relevant peers. We sincerely hope that the system can make better contribution in the field of selling in the next following days.

In future studies, we will aim at using this system and modified the core code in order to adapt the wide potential applications. The existing system we developed is used for the application of medical retails. And after the modification of core codes and the redesign of the software, the system can be extended to various fields in retails. In addition, we will also use the public-key algorithm to replace or combine the AES system in order to test the effectiveness of the systems we developed by making different comparisons.

Acknowledgements

This work was supported by Hebei North University (No. Q2014002,No.ZD201301,No.ZD201302,No.ZD201303,No.Q2014005,No.Q2014008) and the Education Department of Hebei Province(No.QN2014182).

References

[1] J. Rakesh Mohan, International Marketing, **(2008)**.
[2] K. L. Keller and K. Richey, Journal of Brand Management, vol. 14, no. 1, **(2006)**.
[3] K. J. Clancy and P. C. Krieg, "Counterintuitive Marketing: Achieving Great Results Using Common Sense, Simon and Schuster", **(2001)**.
[4] M. Brezis, Israel Journal of Psychiatry and Related Sciences, vol. 45, no. 2, **(2008)**.
[5] C. B. Sufrin and J. S. Ross, "Obstetrical & Gynecological Survey", vol. 63, no. 9, **(2008)**.
[6] J. Barfett, B. Lanting and J. Lee, McGill J Med, vol. 8, no. 1, **(2004)**.
[7] C. S. Landefeld and M. A. Steinman, New Eng. J. Med., vol. 360, no. 2, **(2009)**.
[8] N. T. Courtois and J. Pieprzyk, "Advances in Cryptology-ASIACRYPT 2002", Springer Berlin Heidelberg, **(2002)**.
[9] J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard", Springer, **(2002)**.
[10] W. Stallings, Cryptologia, vol. 26, no. 3, **(2002)**.
[11] J. Schwartz, New York Times, C12, **(2000)**.
[12] J. Daemen and V. Rijmen, AES proposal: Rijndael, **(1999)**.
[13] J. Viega, M. Messier and P. Chandra, O Reilly Media, Inc., **(2002)**.
[14] S. Ahmed, K. Samsudin and A. R. Ramli, Secu. & Comm. Net., **(2014)**.
[15] T. B. Sivakumar, S. Geetha, App. Mech. & Materials., vol. 573, **(2014)**.
[16] M. S. Kumar and S. Rajalakshmi, 2014 2nd Int. Conf. on. IEEE, **(2014)**.
[17] H. Patel, R. O. Baldwin Int. J. App. Cry., vol. 3, no. 2, **(2014)**.

Authors

Jingjing Yang, a lecturer in the School of Information Science and Engineering, Hebei North University, China. His research interests are in the field of medical information and internet of things.

Yuanqiang Wang, a lecturer in the School of Information Science and Engineering, Hebei North University, China. His research interests are in the field of medical information and internet of things.

Xiao Zhang, a Professor in the School of Information Science and Engineering, Hebei North University, China. His research interests are in the field of medical information and internet of things.