International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:12, 2008

Design and Implementation of Secure Electronic Payment System (Client)

Pyae Pyae Hun

***Abstract*—**Secure electronic payment system is presented in this paper. This electronic payment system is to be secure for clients such as customers and shop owners. The security architecture of the system is designed by RC5 encryption / decryption algorithm. This eliminates the fraud that occurs today with stolen credit card numbers. The symmetric key cryptosystem RC5 can protect conventional transaction data such as account numbers, amount and other information. This process can be done electronically using RC5 encryption / decryption program written by Microsoft Visual Basic 6.0. There is no danger of any data sent within the system being intercepted, and replaced. The alternative is to use the existing network, and to encrypt all data transmissions. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. Results In order to be secure the system the communication between modules is encrypted using symmetric key cryptosystem RC5. The system will use simple user name, password, user ID, user type and cipher authentication mechanism for identification, when the user first enters the system. It is the most common method of authentication in most computer system.

***Keywords*—**A 128-bit block cipher, Microsoft visual basic 6.0, RC5 encryption /decryption algorithm and TCP/IP protocol**.**

I. Introduction

INCREASINGLY, people are using computer networks to access and pay for goods and services with electronic money[1]. E-money or digital cash is merely an electronic representation of funds. E-money with a net result of funds transferred from one party to another[2].The primary function of e-cash or e-money is to facilitate transaction on the network. E-money is a necessary innovation in the financial markets[3].

In electronic payment system, server stores records of every transaction. When the electronic payment system eventually goes online to communicate with the shops and the customers who can deposit their money and the server uploads these records for auditing purposes.

This system includes two main parts: client module and server module. This paper presents the tasks of the user interface module for client. The purpose of this module is to pass request made by client to server which stores all transaction information in a set of data files. The server site would respond by sending all the items of the client requests. The client process also contains solution-specific logic and provides the interface between the user and the rest of application system. The user interface module and the server module communicate using TCP/IP protocol.

This paper deals with the implementation of client/server database for secure electronic payment system. Database management system (DBMS) is a computer program, which serves as a tool for storing data in a database for retrieving information from it and for keeping it up to date. DBMS is very helpful to all users who want to input large amount of information and vast amount of calculations at the same time[4].

To be secure electronic payment system, it is used cryptography which can protect conventional transaction data such as account number, amount and other information. To most people, cryptography is concerned with keeping communication private[5]. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history RC5 algorithm is used for data encryption and decryption which can provide confidentiality and security. Microsoft Visual Basic 6.0 is used to implement this system.

II. Overview of the System

This system is designed on Client/Server architecture that is developed on the windows and network groups. This system includes two main parts which are user interface module and server module. This thesis presents the user interface module. Modules of secure electronic payment system can be shown in Figure 1. The purpose of this module is to pass request made by client to server. The server stores all transaction information in a set of data files. There are different types of clients that are customers and shops who own the shop owners.

The communication between the client and server is TCP/IP protocol. Database management system serves as a tool for storing data in a database for retrieving information from all users in this system. To be secure this system, symmetric key cryptosystem RC5 is used to protect conventional transaction data such as account numbers, amount and other information.

The author received her CHT(Computer Hardware Technology) degree from University of Computer Studies, Yangon (UCSY).She is presently at "Material Science and Material Engineering Research Centre" (Ministry of Science and Technology), Kyautse District, Mandalay Division, Myanmar. Her research interest include electronic commerce, software agents, secure electronic payment systems and database management system projects.(pyaepyaehun@gmail.com)

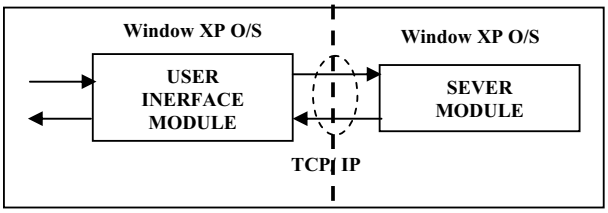

Fig. 1. Modules of Secure Electronic Payment System

This system is secure for the customers and shop owners because it has been designed from the start for the needs of the network. The security architecture of electronic payment system is designed by RC5 encryption/decryption program written by Microsoft Visual Basic 6.0. This system eliminates the fraud that occurs today with stolen credit card numbers. The overview of the secure electronic payment system is shown in Figure 2.

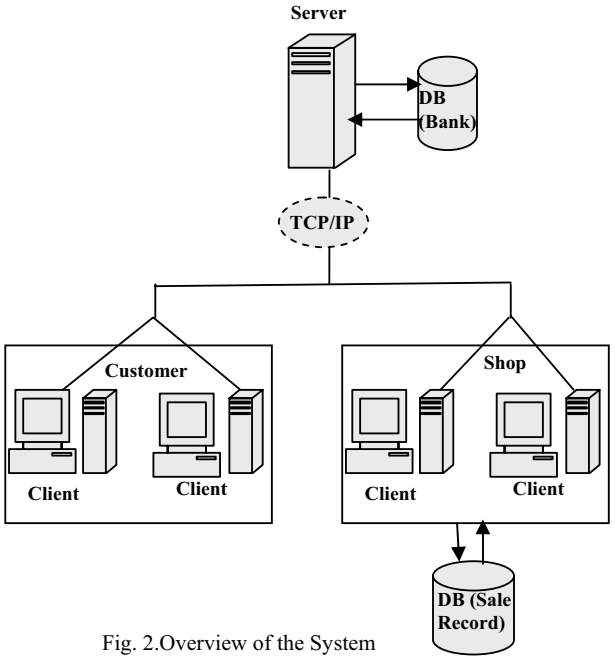

Fig. 2.Overview of the System

III. User Interface for Client Modules

The user interface for client module is a linking process between the customers and the system [6].The user interface takes all inputs for the user, and passes the information to the server to deal with database system. The sole purpose of the user can be seen in the system, and this user interface is the one module where tasks can be controlled under the server. This module is created by use of pull-down menus, buttons, status bars, dialog boxes, and etc. Microsoft Visual Basic 6.0 programming environment allows the programmer to easily make use of all these features without worrying about all the "behind the scenes" coding that must be done in order to make the application run in Window XP. User interface module flow chart is shown in Figure 3 .

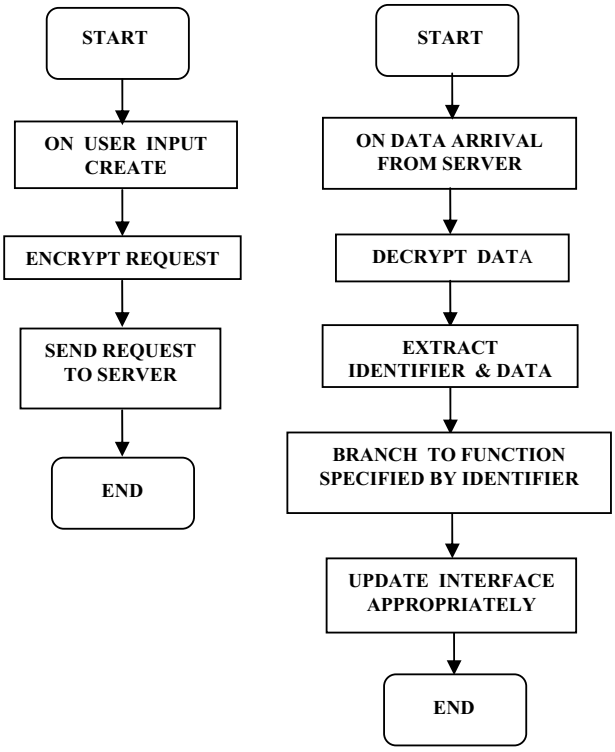

Fig. 3. User Interface Module Flow Chart

IV. System Design

The system design consists of customers and shop owner who owns shops. The client module contains databases which are related to category, goods, purchase details, sales details and shop owner. Figure 4 shows entity relationship diagram for shop details. Figure 5 shows the system design of flow chart.Figure 6 shows data flow diagram for the shop owner process that checks whether member or not. Figure 7 shows data flow diagram for the customer process that checks whether member or not. Figure 8 shows data flow diagram for purchasing goods process by shop owner. Figure 9shows data flow diagram for selling goods process by shop owner. Figure 10. shows data flow diagram for viewing sales details. Figure11 shows data flow diagram for purchasing items by customer. Figure 12. shows data flow diagram for viewing purchase details Figure 13. shows data flow diagram for viewing category details. Figure 14. shows data flow diagram for viewing goods details.

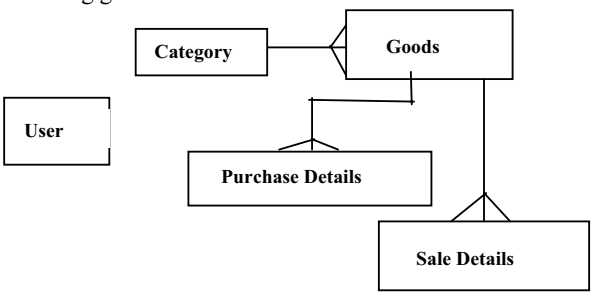

Fig. 4. Entity Relationship Diagram for Shop Details

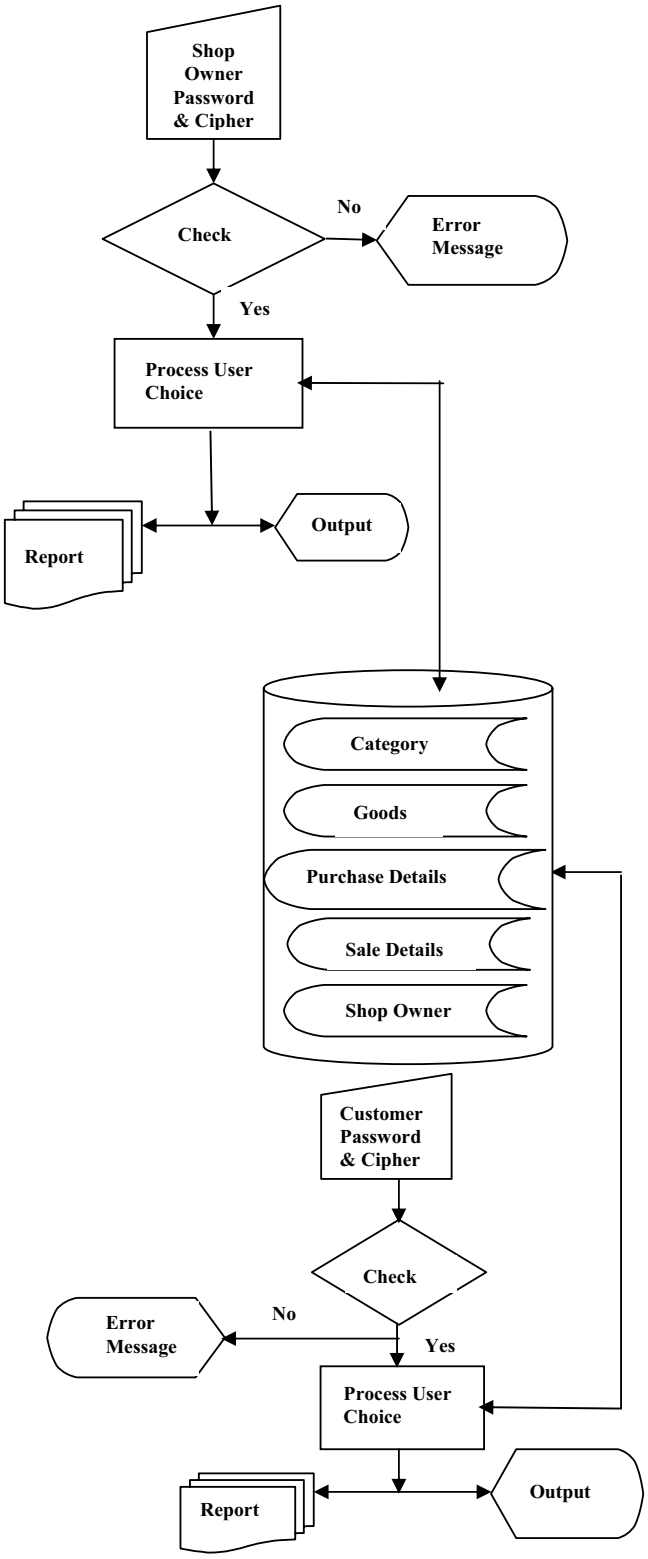

Fig. 5. The System of Flow Chart

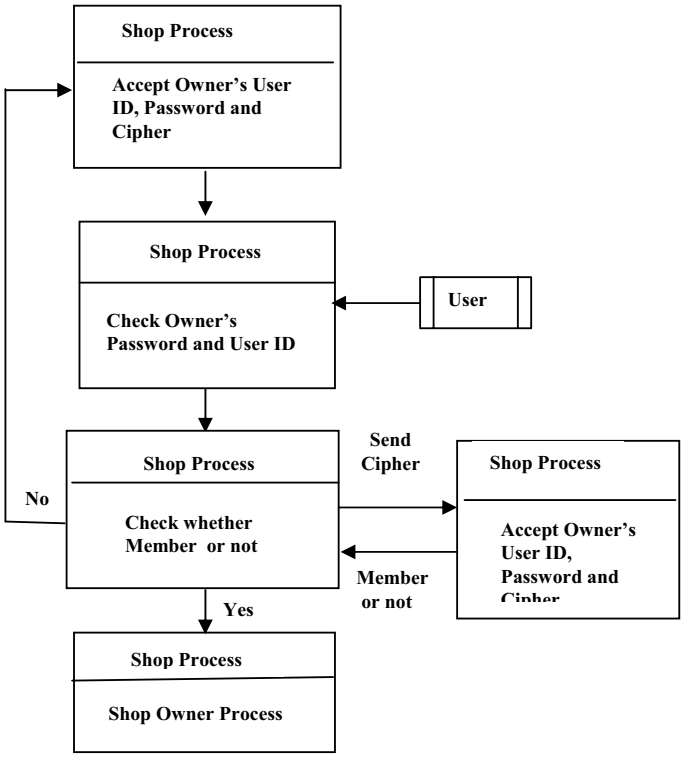

Fig. 6. Data Flow Diagram for the shop Owner Process that Checks Whether Member or Not

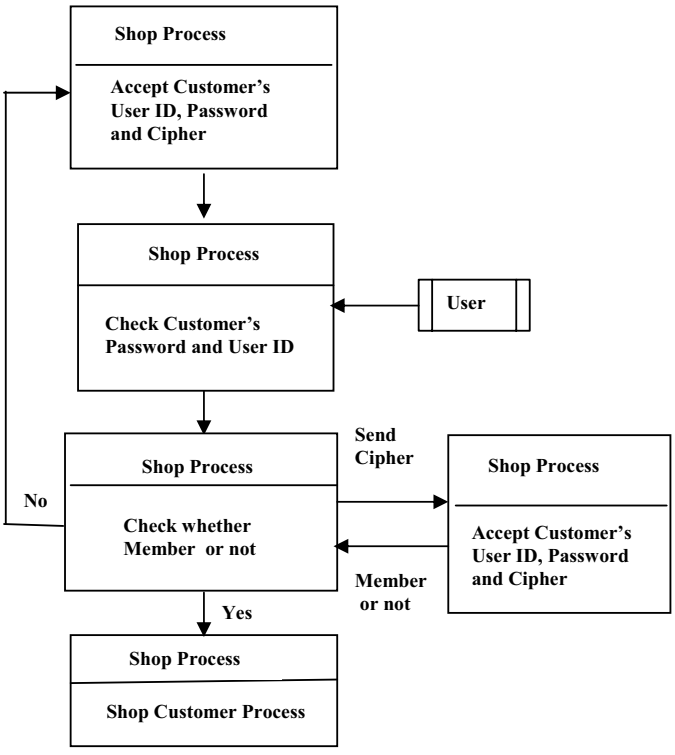

Fig. 7. Data Flow Diagram for the Customer Process that Checks Whether Member or Not

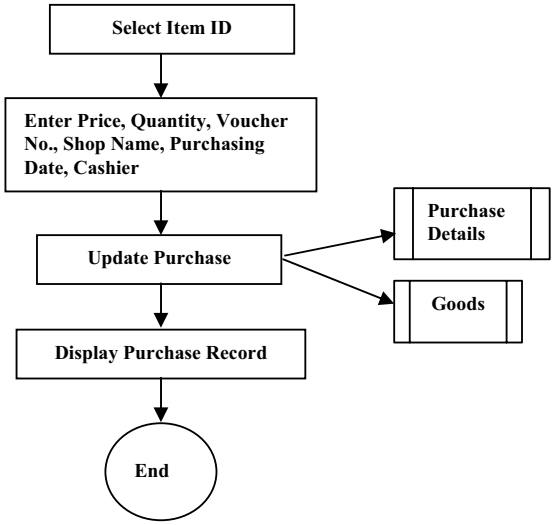

Fig. 8. Data Flow Diagram for Purchasing Goods Process by Shop Owner

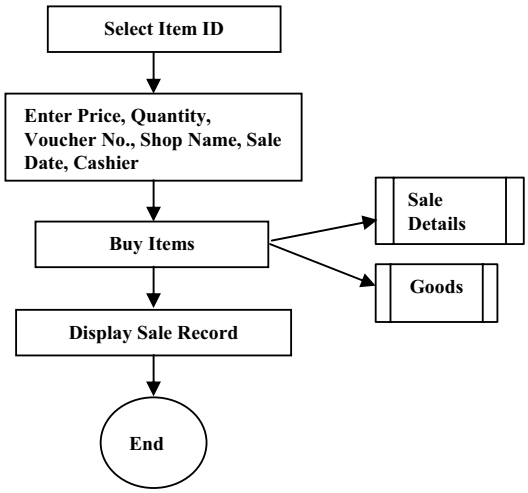

Fig. 9. Data Flow Diagram for Selling Goods Process by Shop Owner

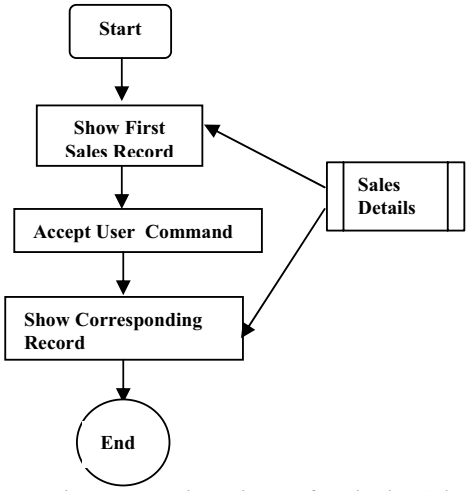

Fig. 10. Data Flow Diagram for Viewing Sales Details

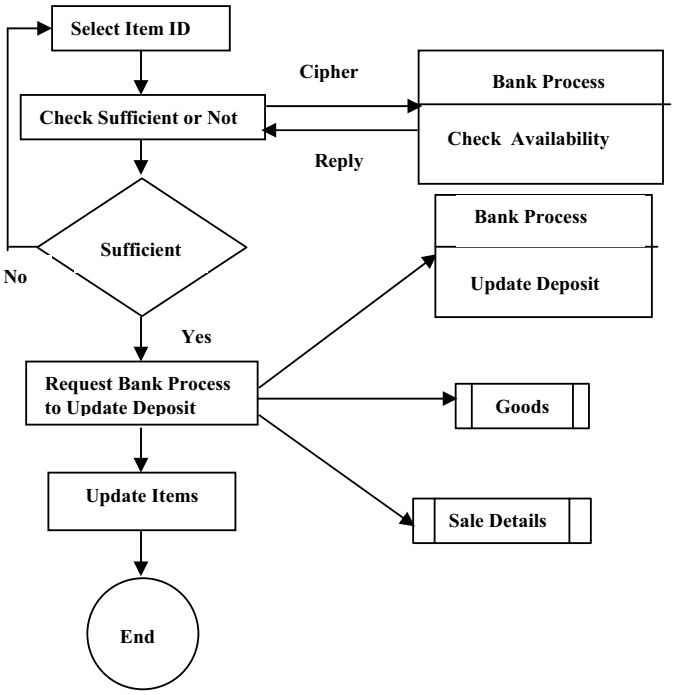

Fig. 11. Data Flow Diagram For Purchasing Items By Customer.

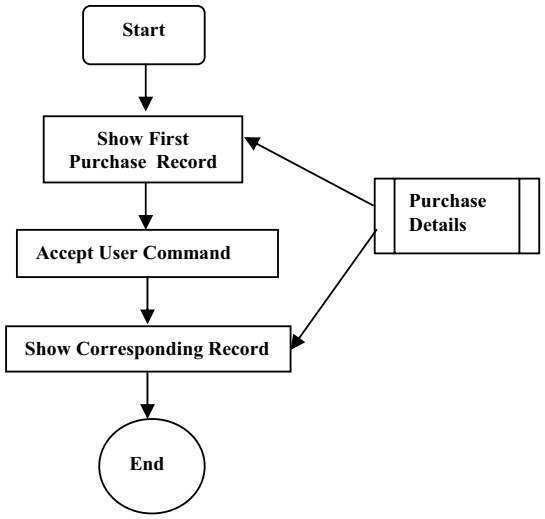

Fig. 12. Data Flow Diagram for Viewing Purchase Details

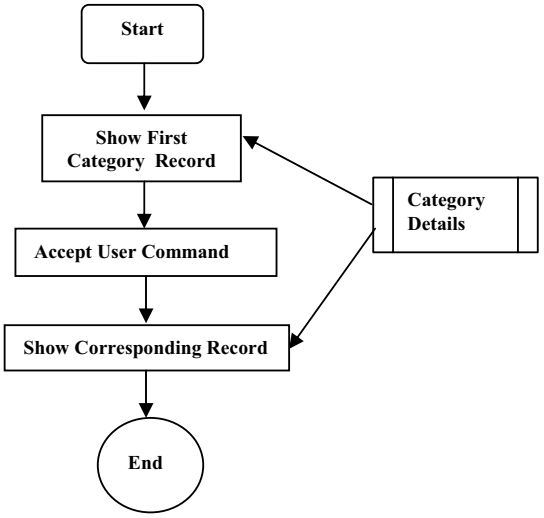

Fig. 13. Data Flow Diagram for Viewing Category Details

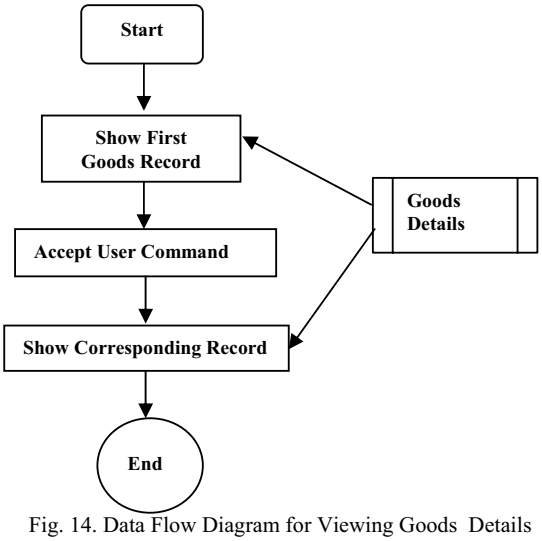

Fig. 14. Data Flow Diagram for Viewing Goods Details

V. Database Design

The client module contains local databases which perform the shop transaction. The local database are category, goods, purchase details, sale details and user that are shown in the following tables.

(1) Category : Table

No.	Field Name	Data Type	Descriptions
1.	Category ID	Text	Category Number (C001,…etc)
2.	Category Name	Text	Medicine and Other Item Groups
3.	Descrip-tion	Text	Item groups that are collected the similar items

(2) Goods: Table

No.	Field Name	Data Type	Descriptions
1.	Item ID	Text	Item ID (i0001,…etc)
2.	Item Name	Text	Items name that can sell in the shop
3.	Category ID	Text	Category Number (C0001,…….etc.)
4.	Quantity per Unit	Text	Quantity in one unit
5.	Unit Price	Money	Price of items
6.	Unit in Stock	Text	The rest stock in the shop
7.	Supplier	Text	The person's name who sells the items

(3) Purchase Details: Table

No.	Field Name	Data Type	Descriptions
1.	Voucher No:	Auto No:	Voucher Number (V123,……..etc)
2.	Cashier	Text	Cashier Name who sell the items
3.	Purchase Date	Date/Time	Date who purchase the items
4.	Item ID	Text	Item ID that are labeled items
5.	Number of Units	Text	Number of Units
6.	Unit Price	Money	Price of items
7.	Supplier	Text	A person who sell the items

(4) Sale Details: Table

No.	Field Name	Data Type	Descriptions
1.	Sale ID	Text	Sale Number (1,2,3,…..etc)
2.	Voucher No:	Auto No:	Voucher Number : (1,2,3,……etc)
3.	Cashier	Text	Cashier Name who sell the items
4.	Sale Date	Date/Time	Date which sells the items
5.	Item ID	Text	Item Number : (1,2,3,……..etc)
6.	Number of Unit	Text	Number of Units
7.	Price	Money	The value of price
8.	Customer ID	Text	Customer ID who purchase the items.
9.	Shop Name	Text	The name of shop that sell the items

VI. RC5 IMPLEMENTATION

The use of RC5-32/12/16 is the "normial version". RC5-32/12/16 has 32 bit words(64-bit plaintext and ciphertext blocks), 12 rounds in the encryption and decryption algorithms, and a key length of 16 bytes (128 bits) [7].

In this case, 32 bit words(a long data type),10 rounds in the encryption and decryption algorithms and a key length of 16 bytes(128 bits) are used.

The word size can be chosen. When the number of loop is chosen as r =1, the subkey will appear as the formula t = 2r+2. In the crypto calculation dialog box, "SUBTRACTION", "ADDITION", "LEFT SHIFT", "RIGHT SHIFT", "BINARY", "AND", "OR", "XOR", "SUBKEY" and "RC5 encryption/decryption" can evaluate.

If someone does not know RC5 algorithm, he can learn by pressing "HELP" button. In the "HELP", the details of RC5 are explained. If someone want to see the previous page, the "previous" button is clicked. If someone does not see the current page, he can "close" button.

Decimal or binary value can be chosen. Similarly, "AND","OR" , "XOR", and "subtraction" can be calculated. If someone wants to know the binary value of 10, he can choose the binary button.

(a) Key Expansion

RC5 is a family of encryption algorithms determined by three parameters. They are w , r and b . "w" means word size in bits that RC5 encrypts 2-word block. "r" means the number of rounds. "b" means the number of 8-bit bytes (octets) in the secret key K. [9]

Two subkeys are used in each round, and two subkeys are used on an additional operation that is not part of any round, so t=2r+2. Each subkey has one word (w bits) in length. The subkeys are stored in a t-word array labeled S[0],S[1],-----,S[t-1]. Using the parameter r and w as inputs, for example, "aung" as input, this array is initialized to a particular fixed pseudorandom bit pattern. Then the b-byte key, K[0, -----, b-1], is converted into a c-word array L[0 ,----- ,c-1].

Finally, a mixing operation is performed that applies the contents of L to the initialized value of S to produce a final value for the array S. The initialized array S is mixed with the key array L to produce a final array S of subkeys. The key expansion function has a certain amount of one-wayness : It is not so easy to determine K from S. Figure 15. shows RC5 Key expansion.

(a) Encryption of the System

RC5 uses three primitive operations such as addition, bitwise exclusive-OR, and left circular rotation. The plaintext is assumed to initially reside in the two w-bit registers A and B.

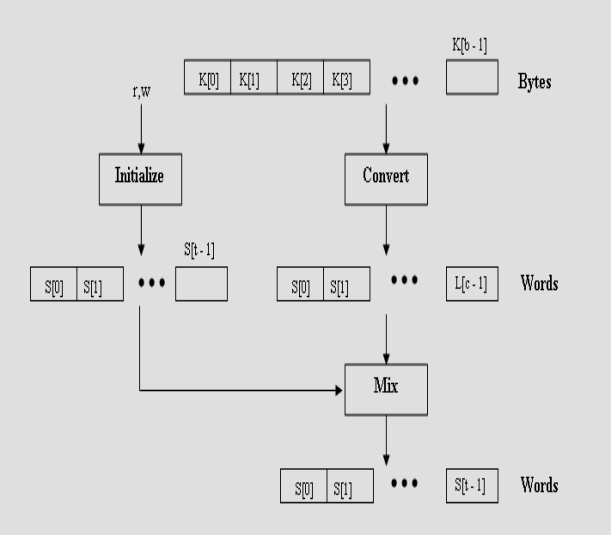

Fig. 15. RC5 Key expansion[8]

For example, the plaintext is B0001. After 10 rounds has completed, the resulting cipher text is contained in the two variables LE_{10} and RE_{10}. Each of the 10 rounds consists of a substitution using both words of data, a permutation using both words of data.

By running RC5 encryption program written by Visual Basic, the ciphertext 3FD1F35FOA87 is obtained as shown in Figure 16. Both halves of the data are updated in each round. RC5 encryption program is used for other data which are sent to server. Thus, one round of RC5 is somewhat equivalent to two words of DES.

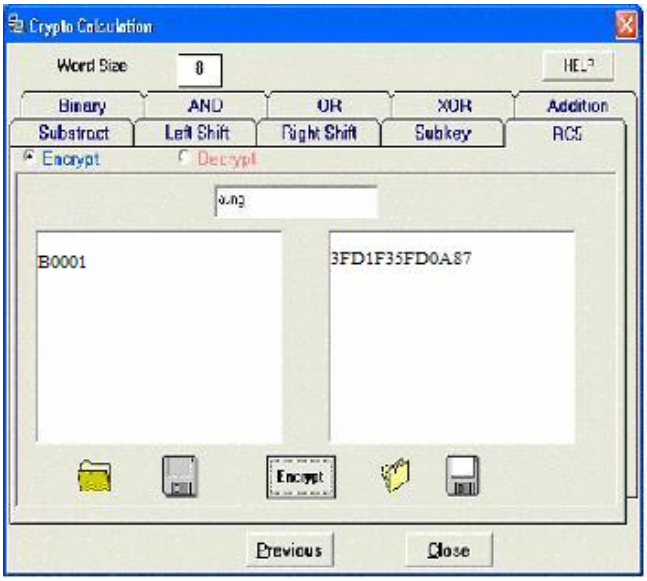

Fig. 16. RC5 Encryption from Crypto Calculation

(c) Decryption of the System

Decryption is easily derived from the encryption algorithm. In this case, the 2w bit of the ciphertext (for

example, 3FD1F35FOA87) are assigned to the two one-word variables. The variables LD_{10} and RD_{10} refer to the left and right half of the data before round 10 has begun, where the rounds are numbered from 10 down to 1.

Finally, the original plaintext B0001 can be obtained. RC5 decryption program is used for other encrypted data which are sent from client and server. The rotations are the only nonlinear portion of the algorithm. The amount of rotation varies depending on the value of data moving through the algorithm. Linear and differential cryptanalysis should be more difficult. Figure 17 shows RC5 decryption from crypto calculation.

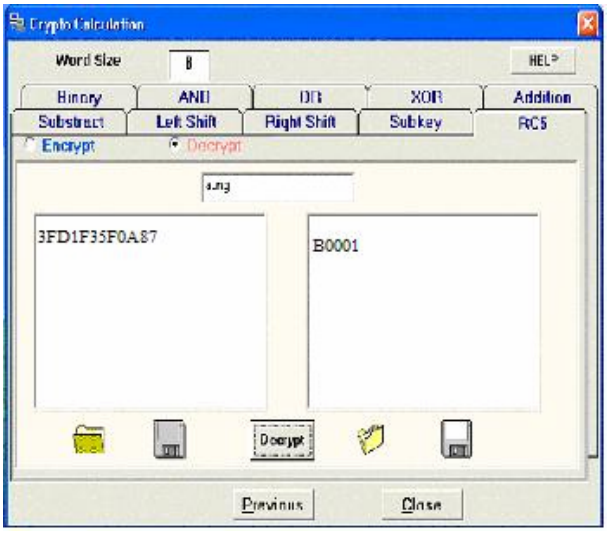

Fig. 17. RC5 Decryption from Crypto Calculation

VII. IMPLEMENTATION OF THE SYSTEM

The layout of the user interface application is designed to be as user friendly as possible. When the user opens the software, the title form and the main application will appear. If the user clicks the “next” button, the login for shop dialog box will appear. If the user presses “close” button, the software will be terminated. The first user must be shop owner who can access the shop process.

(a) Login for Shop

In this form, the user must enter the user name, user ID, password and cipher for authentication as shown in Figure 18.The first user must be shop owner to access her shop. She must enter words as the cipher which can be obtained by running the RC5 encryption program for security. And then click the “OK” button. If authentication had been successful, the user can use the system.

Otherwise, the system will display a message box that informs the user who is not a member. The user can quit this form by clicking the “cancel” button. After authentication has been successful, the system displays "Welcome to Chit Sayar Shopping Center" and then secure electronic payment system window will appear. This is the “Chit Sayar Shopping Center” who owns by Aye Aye. In this case, there are two shops and ten customers who deposit in the bank from server.

If the server is not running , the client program cannot be opened.

Fig. 18. Design Window of Login for Shop

(b) Secure Electronic Payment System

In this form, there are Customer, Shop owner, Sale Detail Input, Purchase Detail Input, Category Input and Goods Input buttons . If the user chooses "Customer" button, the system displays the menu of “login form” for customers. If the user chooses "Shop Owner" button, the system displays the menu of “purchase” window. If the user chooses "Sale Detail Input" button, the system displays the “Sale Detail” Window. If the user chooses "Purchase Detail Input" button, the system displays the “Purchase” Window. If the user chooses "Category Input" button, the system displays the menu of “Category” Window. If the user chooses "Goods Input" button, the system shows the menu of “Goods” Window.

User will only be able to enter windows that they have access too. And users deposit money to their account in bank from server.

(c) Customer Login Window

If the user chooses the “Customer” button, the “Login Form” dialog box will appear. This login form dialog box consists of a prompt for the customers “User Name”, “User-ID”, “Password” and “Cipher” which is used authentication. There is also a “cancel” button, and an “OK” button. The “cancel” button can be used to exit the application, and the “OK” button can be used to send the user name and password, the user type and cipher to the server for authentication. Cipher can be implemented by running RC5 software written in Microsoft Visual Basic 6.0. If the user enters the correct password, the customer window will appear, otherwise the application will exit.

For security and authentication, if the customer may fill the wrong entry, the error message will appear. If a person fills the wrong entry, the error message will appear. The new customer can add to server. The deposit amount of customer

can add to bank from server. Figure 19. shows the error message for wrong entry.

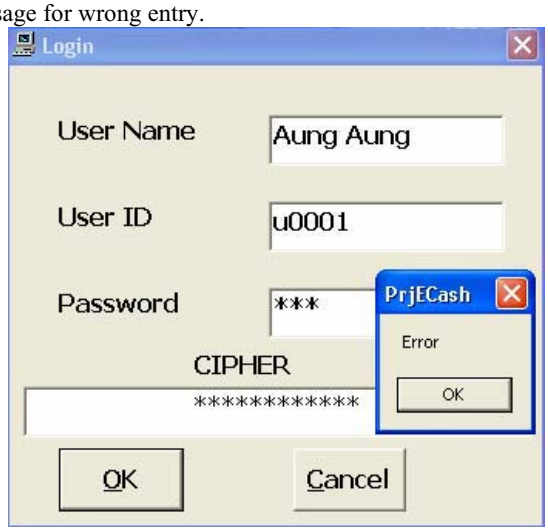

Fig. 19. The Error Message for Wrong Entry

(d) Customer Window

The customer window has two pages: the "Selling Goods" page and "Query and Report" page.

The "Selling Goods" page is used to buy the desired items from the shop. The customer can choose the desired items from item list. For example, if i0012 is selected from item list, the system will display item name and item price. The customer can fill the desired quantity. And "Buy Item" button is pressed. The selected item-ID, item price, quantity(Qty) and cost can be displayed on the table. The customer can choose other items. The total result is shown on the table. When the "OK" button is selected, the cost will be subtracted from customer's account by the system. If the sale item quantity is more than remain goods quantity, the error message will be shown.

The "Query and Report" page contains "Query on Voucher Number", "Query on Sale Date" and "Query on Sale". The shop owner and the accountant can check the sale and the sale amount on desired date, When the desired voucher number is selected, sale ID, voucher number, cashier name who sell the items, item ID, number of quantity, price, customer ID who purchase the desired items and shop name can be traced. By selecting "Query on Voucher Number" , the desired voucher number can be traced.

(e) Purchase Window

When the "shop owner" button from the secure electronic payment system is selected, purchase window will appear. This window contains purchase page and query page.

The "purchasing" page is used to purchase and added the required items for shop. For example, when i0001 is selected from item list, the system displays item ID, item price, and the required quantity is filled by customer. Other items can be selected. When "Add Item" is pressed, item ID, item name, price, quantity (Qty) and cost can be seen on the table. The purchase total amount is shown under the table. After pressing "OK" button, the purchasing goods quantity will be added to the remain goods or items.

The "Query" page contains "Query on Voucher Number", "Query on Purchase Date" and "Query on Purchase". The shop owner and accountant can check the purchase amount on the desired date. When the desired purchase date is selected, purchase ID, voucher number, cashier name, purchase date, item ID, quantity , price and supplier can be traced. By selecting "Query on voucher number", the voucher number can be traced and checked. If sale items quantity is overflowed more than remain goods quantity, the error message will display.

VIII. Conclusion

In our secure electronic payment system that the authorized owner can use this system reliably as he is an administrator and can only change the data. He will be able to know the desired reports and other management activities. The customers will be able to purchase the desired items securely without taking the money which can be stolen by snatcher or pick-pocket.

Acknowledgment

I would like to express my heart-felt thanks to Dr. Win Aye, Pro-rector, Computer University (Mandalay) for supporting me so that pursue my research. Next I would like to thank U Kyaw Zwa Soe, Pro-rector, University of Computer Studies,Yangon (UCSY) and Professor Daw Nwe Ni,(UCSY),for their continuously providing with inspiration and their guidance during the period of the paper.

References

[1] Ferche,A., Wrightson, G., Computer Money , Heidelberg: Dpunkt, 1996
[2]"Cheque system on line electronic payment " http://www.cict.dtu.dk/upload/centre/cict/publications/working%20papers/cti wp39.pdf
[3] "Achieving Electronic Privacy" htt://www.digicash.com/publish/sciam.html
[4] Date,C.J, "An introduction to Database System", ISBN 0-201-824582,Seventh Edition, The System Programming Series, Addison-Wesley Publishing Company,1994
[5] Yin, Y. "The RC5 Encryption Algorithm: Two Years On. " Crypto Bytes, Winter 1997.
[6] Ben M^{c} Fadyen, UNICASH: A Digital Cash System , Department of Computer Science and Electrical Engineering, The University Queensland.
[7] Kaliski Jr, B.S. and Yin, Y. L., September 1998. "On the security of the RC5 Encryption Algorithm" , 2006.
[8] W. Stallings, 1998. "Cryptography and Network Security", Third Edition, 2006 .
[9] R.L.Rivest, R.March 1997. "The RC5 Encryption Algorithm" . MIT Laboratory for Computer Science, 545 Technology Sure, Cambridge, Mass, 1996.