A Data Mining Technique for a Secure Electronic Payment Transaction

Vipin Saxena
Department of Electrical and Computer Engineering
Doorfontein Campus, University of Johannesburg
P.O. Box 17011 Doornfontein 2028, Johannesburg, South Africa
E-mail:vsax1@rediffmail.com

N.M.P. Verma
Department of Economics
Babasaheb Bhimrao Ambedkar University
(A Central University)
Vidya Vihar, Rae Bareli Road, Lucknow (U.P.) – 226025, India
E-mail: nmpverma@rediffmail.com

Ajay Pratap
Department of Computer Science
Babasaheb Bhimrao Ambedkar University
(A Central University)
Vidya Vihar, Rae Bareli Road, Lucknow (U.P.) – 226025, India
E-mail: pratap_aj@yahoo.co.in

Abstract

Due to the evolution of the Electronic Learning (E-Learning), one can easily get desired information on computer or mobile system connected through Internet. Currently, E-Learning materials are easily accessible on the desktop computer system, but, in future, most of the information shall also be available on small digital devices like Mobile, PDA, etc. Most of the E-Learning materials are paid and customer has to pay entire amount through credit/debit card system. Therefore, it is very important to study about the security of the credit/debit card numbers. The present paper is an attempt in this direction and a security technique is presented to secure the credit/debit card numbers supplied over the Internet to access the E-Learning materials or any kind of purchase through Internet. A well known method i.e. Data Cube Technique is used to design the security model of the credit/debit card system. The major objective of this paper is to design a practical electronic payment protocol which is the safest and most secured mode of transaction. This technique may reduce fake transactions which are above 20% at the global level, al beit, it shows a declining trend in the recent past.

Keywords: E-Learning Material, Security, Electronic Transaction, Data Cube Technique, Credit/Debit Card

Introduction

The rapid growth of internet services has changed the economical, cultural and social activities. In most of the countries, people are using these services for sale and purchase. Day-by-day, companies are hosting the web pages on the server which is connected through the autonomous computer systems. The arrangement of the computer systems is according to the distributed computer system, in which customers or consumers can access the server and this connectivity is having the high class of bandwidth. **Electronic Commerce** popularly known as **E-Commerce** is a new way to do business transactions electronically. Electronic transaction is a very important part of E-Commerce and therefore a very secured electronic transactions are required. A Secure Electronic Transaction (SET) is a system which ensures the security of financial transactions on the Internet. Electronic money (e-money) or digital cash (e-cash) is merely an electronic representation of funds. E-money is observed with a net result of funds transferred from one party to another. 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. This may become popular in the era of globalization and very fast economic activities and transactions.

The electronic payment system has two major components: The client module and the server module. The connectivity between these two modules is defined as interface module and generally known as user interface module for client. The objective of this module is to send the request from client to server. This module will store all transaction information in the form of data cubes. The user interface module and the server module communicate with each other using TCP/IP protocol. Let us now describe some of the important references related to security of the electronic payment system.

Authentication techniques and their implications are discussed by (Stallings, 1998 and 2006). The conventional cryptographically techniques are given in this book. The protocols for the authentication method are explained by (Syversion & Cervesato, 2000). Computing inverse of a shared secret modulus involving mathematical formulation of RSA algorithm is discussed in (Catalano et al., 1999). The sensor networks are very popular nowadays for the wi-fi connectivity of the computer systems; therefore, the security system like cryptosystem for sensor networks is needed and studied by (Szewczyk et al. 2001). The strength of RSA algorithm is discussed by (Fujisaki et al., 2002). This algorithm is used for securing the digital signature for on-line transaction of the information. Security proofs which can be implemented for various digital signature schemes are studied by (Pointcheval and Stern, 1996). In the literature, it is found that various fast RSA implementations through practical demonstration are described in (Kaya Koc, 1994). Electronic commerce for financial services Industry: Account Based Secure Payment Objects are described by (DSTU, 2000). The other references related to the digital security system are (Krishnamurthy et al. 2002, Wayner et al. 1997, Web Pages www.cict.dtu.dk, www.digicash.com). The new directions in the cryptographic system are given by (Diffie and Hellman, 1978). The popular RSA algorithm is designed by (Rivest et al. 1978). In this paper, the basic of RSA algorithm and other issues related to cryptography are discussed.

In the present work, transactional information is saved in the form of Online Analytical Processing (OLAP) Data Cubes for secure and reliable Electronic Payment System (EPS). The flow of credit card number from customer computer system to the server must be secured for which a cryptography algorithm is used. The algorithm is called as Rivest, Schmidt and Adelman (RSA) algorithm, which is a type of Public-key Cryptosystem, for electronic payment which can provide confidentiality and security. It uses a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one is known as public key. A case study of Credit Card System is demonstrated after designing the model through design of data cubes. The whole study is based upon the concept of the prime numbers which are generated automatically through the above approach.

Methodology

Let us first describe the Client/Server architecture model in which Client or Customer's computer system is connected through network with the Server. The number of customers are connected through the network called as the Internet and the architecture is based on the distributed computing system i.e. individual client has sufficient hard disk space and random access memory to run the application on its own computer system. The client and server can communicate with each other using TCP/IP protocol. The connectivity between the client and server computer systems is shown in Figure 1. After getting the connectivity with server computer system, client is able to fetch any kind of information which are available in the form of web pages i.e. client is able to access the E-learning materials. For this Online Analytical Processing (OLAP) is done i.e. OLAP system serves as a tool for storing data and for retrieving information from all users in this system. For accessing the information from server, customer has to supply his credit/debit card number alongwith PIN on the internet only if the services are paid. The searching and sorting of the databases available on the computer systems are faster if one uses the Data Cubes methodology. Various steps for OLAP are described below:

Step 1:

The first step is to store the customer information in the form of data cubes. When the user enters his/her credit/debit card number or account information on the web page then this information first is stored in the form of OLAP data cubes as represented below in Figure 2. Online Analytical Processing (OLAP) products are developed to store these transactional data for easy retrieving. It helps for the system analysts to do decision support on historic transactional data. They expose a multidimensional view of the data logically with numeric attributes like sales, amount and revenue forming the measures or cells of the multidimensional cube. In figure 2, the credit/debit card of the customer consists of three major attributes namely “CREDIRCARD_NO”, “CUST_NAME”, and “BANK_NAME” which are taken along x, y and z axes, respectively for credit card number, customer name and bank name.

Step 2:

On the basis of step 1, let us create N records of the customers and these customers desire to access E-learning materials or want to purchase the product. This information as per the designed data cubes for the attributes are given in Table 1. The table is normalized and primary key is the CREDITCARD_NO while the secondary key is the CUST_NAME as represented in the table. This information is designed with the help of data cubes which is shown in Figure 3.

Step 3:

Now we want to secure the supplied credit card numbers through an algorithm known as RSA algorithm. For this purpose, a constant 'bitstrength' is used, which is the size of the RSA modulus in bits. The algorithm is based upon the computation of the encryption and decryption keys which are relatively primes and used to secure the credit card numbers. The sub steps are given below:

Select the two prime numbers p and q;

Compute n=p*q and Φ(n) = (p- 1)*(q-1);

Compute the decryption key also known as private key defined as d such that gcd(d, Φ(n))=1, where gcd() shows the greatest common divisor of two numbers;

Now compute the encryption key also known as public key defined as e such that ed*mod(Φ(n))=1, where mod is the remainder.

The algorithm is partially based on modular algorithm and multiplicative inverse is one of the properties of it. If we have an integer e in the range of [0, n-1] then it is possible to find a unique integer d in the range [0, n-1].

Step 4:

After step 3, we have two keys, encryption and decryption keys e and d, respectively. Now, the credit card number of the customer is treated as the plain text defined as P and initially this credit card number is encrypted as shown in Figure 4. The plain text is converted into the cipher text represented as C and it is given by

$$C = P^{e} \bmod n \qquad (1)$$

The file to encrypt is processed as a group of strings each containing the specified number of characters and each character in such a string is converted to its ASCII code. After performing the encryption we get the value of C, which is used as an input for the decryption process.

Step 5:

After step 4, the cipher text C is to be decrypted so that one could get again the Plain Text P which shows that the credit card number is successfully reached at the server computer system for secure transaction. The plain text i.e. original credit card number is obtained by

$$P = C^{\mathbf{d}} \bmod n \qquad (2)$$

The process of decryption is shown in Figure 5. The above steps are based upon the concept of the prime numbers. The computations involved for the above steps are for prime numbers which become very large for small values of the prime numbers as shown in the next section.

Experimental Study and Discussion

Let us start the experimental study by considering the credit card number and we have to perform the above five steps. Suppose the credit card number of the customer is 6220218920900012593 as shown in the Table 1 after applying the above steps 1 and 2. For the step 3 and for the security of the credit card number over the Internet, let us compute the encryption and decryption as computed below:

Assume the two small prime values for demonstration of the result i.e. p = 3, q = 11, therefore, n = p*q=3*11=33 and Φ(n) = (p- 1)*(q-1) = (3- 1)*(11-1) = 2*10 = 20;

Now let us compute the encryption and decryption keys e and d, respectively. From step 3(c) gcd(d,20) = 1 and select d=7 so that gcd(7,20) = 1. Now, we have to choose the value of e such that e*d mod Φ(n) = 1 as per step 3(d). Therefore, 7e*mod (20) = 1 and it is valid when e=3. The complete encryption and decryption technique is shown in Table 2 in which original credit card number is supplied by the customer or consumer or client on the Internet and whether it is reached safely at the server computer machine for which two keys i.e. public and private keys are used as shown in the table. The credit card number (6220218920900012593) supplied by the customer is used as a value of P for each digit and then after performing encryption and decryption similar digits are obtained at receiver's end i.e. Server -end which shows that credit card number reached safely.

4. Concluding Remarks

From the above analysis, it is concluded that Data Cube designing method is one of the most power tools for storing the large database of any organization and it gives simplicity for searching and storing the database. In the present work, the number of credit card numbers of the customers are stored in the data cubes and then transmitted over the network. The Client and Server Computer Systems exchange the private and public keys for security of the credit card numbers supplied for the payment over internet. In our secured e-payment system communication between the client and the server are communicating with each other using RSA algorithm as described above, which uses two different keys, public and private keys, to encrypt and decrypt the data. Since both keys are different so it is more secure as compared to other conventional cryptographical algorithms.

References

"Achieving Electronic Privacy" htt://www.digicash.com/publish/sciam.html.

"Cheque system on line electronic payment" http://www.cict.dtu.dk/upload/ centre/cict/ publications/working%20pape rs/cti wp39.pdf.

Adrian Perrig, Robet Szewczyk, Victor Wen, David Culler and J.D. Tygar. (2001). *SPINS: Security protocols for sensor networks*, Mobile Computing and Networking, Rome, Italy.

American National Standard DSTU X9.59, Electronic Commerce for Financial Services Industry: Account Based Secure Payment Objects, 2000.

Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang. (2002). An efficient implementation of multi-prime RSA on DSP processo*r*, University of Texas, Texas, USA.

Cetin Kaya Koc. (1994). *High speed RSA implementation*, RSA Laboratories, CA.

Dario Catalano, Rosario Gennaro and Shai Halevi. (1999). Computing inverse over a shared secret modulus, *IBM T. J*. Watson Research center, NY, USA.

David Pointcheval and Jacques Stern. (1996). Security proofs for signature schemes, *EUROCRYPT '96*, Zaragoza, Spain

Elichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval and Jacques Stern. (2002). RSAOAEP is secure under the RSA assumption, *Journal of Cryptology*.

P. Wayner. (1997). Digital Cash: Commerce on the Net, 2nd Edition, Morgan Kaufmann Publishers, March.

Paul Syversion and Illiano Cervesato. (2000). *The logic of authentication protocols*, FOSAD'00, Bertinoro, Italy.

R.L. Rivest, A. Shamir, and L.M. Adleman. (1978). "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, volume 21, pages 120-126, February.

W. Stallings. (1998). "Cryptography and Network Security", Third Edition, 2006.

W.Diffie and M. Hellman. (1978). "New Directions in Cryptography". *IEEE transactions on Information Theory*. IT-22.472-492.

Table 1. Customer's Credit Card Information

CREDITCARD_NO	**CUST_NAME**	**BANK_NAME**
4514251635485625462	VIPUL SINHA	SBI, LUCKNOW
9546254563521456215	R.K.SINGH	IDBI, KANPUR
6220218920900012593	S.K.AWASTHI	PNB, LUCKNOW
7852312589654852123	RICHA SRIVASTAVA	SBI, LUCKNOW
7502156024500564521	RAJAT TONDON	BOI, VARANASI

Table 2. Encryption and Decryption of the Credit Card Number

Digits of Credit Card (P)	Encryption Module		Decryption Module	
	P^3	P^3 mod 33=C	C^7	C^7 mod 33=P
6	216	18	612220032	6
2	8	8	2097152	2
2	8	8	2097152	2
0	0	0	0	0
2	8	8	2097152	2
1	1	1	1	1
8	512	17	410338673	8
9	729	3	2187	9
2	8	8	2097152	2
0	0	0	0	0
9	729	3	2187	9
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
1	1	1	1	1
2	8	8	2097152	2
5	125	26	8031810176	5
9	729	3	2187	9
3	27	27	10460353203	3

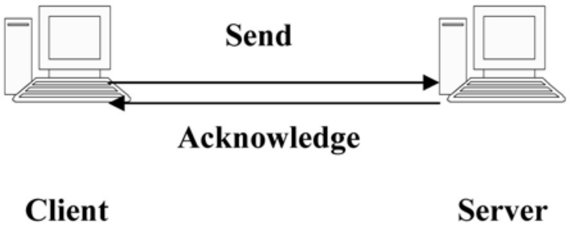

Figure 1. Client/Server Computer Architecture Model

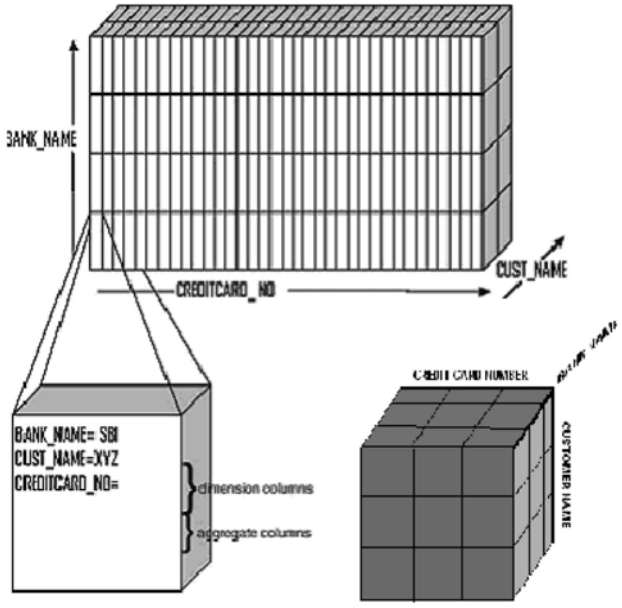

Figure 2. Three Dimensional View of Customer's Information for OLAP

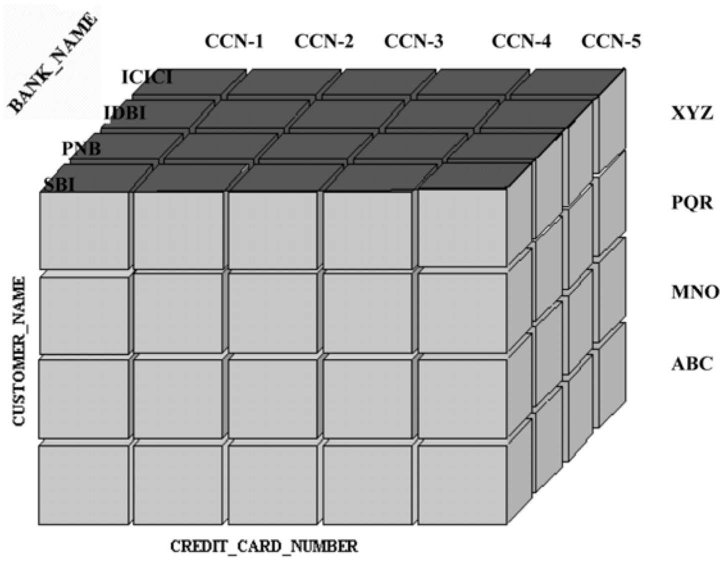

Figure 3. Data Cube Representation of Customer's Credit Card Information

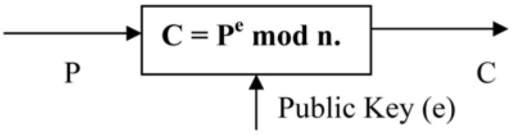

Figure 4. Encryption of Credit Card Number

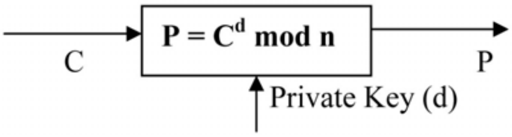

Figure 5. Decryption of Credit Card Number