

A Prototype Design for DRM based Credit Card Transaction in E-Commerce

Sanjay Banerjee¹, Sunil Karforma¹

¹Department of Computer Science, University of Burdwan, Golapbag, Burdwan – 713104, WB, India

Abstract

In E-Commerce credit cards gained popularity as a sophisticated payment mechanism. With the increase in credit card use on web, credit card fraud has gone up dramatically. Which cause customer's inconvenience and for merchant, loss of customers. To combat credit card fraud and to regain the customer's trust an attempt is made here to design a trust based payment system, in which the customer does not need to disclose his/her credit card number during the transaction, and hence they can feel safe. In this newly proposed system on behalf of the customer the bank or the issuer of the credit card is involved to perform the transaction. This is basically done by generating a single use 'token' by the bank which includes information about the customer, merchant, product, payment amount, date of issue and date of expiry etc. and thereafter wrapped as a DRM package. Among various advantages, one is that only the intended user and the specified application software can open the DRM package using special key. The application, thereafter, will take care of the rights imposed on the 'token' and expires itself after the single use. We have tried an attempt to use UML to design the model of such system, which is the recent trend of software engineering practice.

Keyword: Single-use Token, Credit-Card transaction, DRM, Security

1. Introduction

E-Commerce has the advantage to promote a product to the worldwide customers at a very low cost and with minimum effort. At the time of purchasing products or services on the web there is a need to submit customer's personal information such as credit card numbers and financial data etc. The customers would like to submit the data only when they are confident that their submitted information is secured.

To win customers' trust, the E-Commerce system must be fully aware of the Internet security threats and should be competent enough to avail of the advantages of the appropriate technology to combat them. Encryption can be a way of information protection based on cryptographic algorithms, but this is not sufficient [1]. A significant portion of web users feel uncomfortable to send their respective credit card numbers over the Internet due to the lack of security [2][3][4]. Thus an E-Commerce system which has the required ability to earn confidence of the customer can gain their loyalty also. This in turn offers an opportunity of expanding the businesses by the firms.

Primarily there are two types of credit card transaction:

- Card present
- Card not present

In the card present transaction system the security of the transaction is based on the physical cues [9]. Customers accept the risks of using credit cards in places like departmental stores because they can see and touch the products and make judgments about the store, which is almost absent in case of card not present transaction. The E-Commerce system follows the card not present transaction system.

The risk and the challenges of the trust that discourage the credit card holder to participate in the E-Commerce system [9] are spoofing, interception of sensitive data transmitted online, alteration of data during transaction, denial of services (DOS), overcharging the customers at a higher than the agreed prices and besides all Credit card is not a dependable method of E-Commerce payment system because it is designed to rely only physical signatures for authentication [12].

The present paper has been organized as under:

Section 2 deals with prior research relevant to the security issues of credit card transaction in E-Commerce. Section 3 is devoted to identify the specific objective of our study. In Section 4 we have described the methodology to design the proposed system and finally, conclusions have been drawn in Section 5.

2. Prior research

- During the initial stage of development of the Internet the communication protocols did not include the security aspect [5][6]. In 1994 Netscape [7] developed Secure Sockets Layer (SSL) protocol, which sought to offer a private, reliable connection between client and server computers, in the form of electronic identification called digital certificate.
However, there is a major gap in the security which SSL provides because most implementations do not authenticate the client (i.e., the user).
- To overcome the SSL's shortcomings, in 1997 MasterCard [8], Visa [9], and several other companies developed Secure Electronic Transaction (SET). To use SET, the users first must obtain a digital certificate from a Certificate Authority (CA) which is basically an organization engaged in issuing digital certificate to customers. The obtained certificates thereafter require to be verified by the merchants and banks to confirm the identities of the valid cardholders.
Obtaining a digital certificate is a burden to the customers, specifically for the nontechnical users. Most users will not understand about the importance of it or the extent of benefit arising out of it.
- Without imposing the use of certificates, Visa has created the "Verified by Visa" program, which adds a password based protection approach on the existing credit card based purchases. In some ways, this approach is similar to the digital certificate technology, though it is rather simpler than the previous one.
This mechanism is user-friendly both for the technical and the nontechnical customers. Password based technique is much more familiar authentication method than the digital certificate technique and the registration process is very simple and user-friendly.
But this is not as robust as digital certificate security mechanism appears to be. For more security, Visa cards has recently marketed "Smart Visa Card", which comes with an embedded microchip and requires a special card reader attached to the USB port on the user's PC. The password entry still remains the bottleneck and it invites several limitations of the system.
- The above security protocols use cryptographic approach to minimize the fraud over the web transaction using credit card based purchase. To this direction there is another approach named "Single Use Card Number" [11][12]. The purpose of the single-use card number is also to reduce the fraud. The single-use number is generated by the bank on behalf of the cardholders which is

intended to be used for a single purchase and after that the validity of the card expires. Cardholders can substitute the single-use number by their credit card number and hence can keep the credit card number secret from on-line merchants. Single-use card numbers provide no additional verification to the customer's identity and hence the merchant still remains unprotected, though it can keep the fraud limited. The most prominent examples employing the single-use numbers are American Express [13], Discover, MBNA and Visa's Gift Cards.

- Rubin [11] presents an offline generated 'limited use credit card numbers' to solve the problem. The main idea here is to allow the customer to purchase product or service through Internet without exposing the credit card number. Shamir **Error! Reference source not found.** also designed a similar architecture without requiring changes in the existing web structure.

Findings of the Prior Research

- The transaction system that operates in E-Commerce must be able to authenticate the merchant as well as the customer, in order to gain trust from both sides.
- Transaction procedure should be transparent, reliable and simple, so that technical and nontechnical customers can participate.
- The system should not appear to be a burden to the customer.
- The system must be robust in terms of security and reliability.

3. Objective of the present study

In view of the above findings, the present study seeks to design a transaction management system that would fill the functional deficiency of the present E-Commerce transactions using latest technology. In this scenario the Digital Rights Management (DRM) can be used which offers credit card holders more control over their digital identities [1]. In the present E-Commerce transaction system the credit card holder discloses his/her credit card number along with other personal identity to the merchants in order that the merchants can use such information for single use and for the agreed-upon amount only. That is, it is the customer who distributes his/her right to the merchants. Only DRM ensures that the distributed right is not violated. So, our proposed DRM based credit card transaction system improving the level of trust in E-Commerce.

The Unified Modeling Language (UML) is an Object Oriented system analysis and design paradigm which offers generic prototype design technology developed by Grady Booch, James Rumbaugh, Ivar Jacobson in the Rational Software Corporation [14, 15, 16]. This facilitates graphically visualizing, specifying, constructing, and documenting a system's blueprints. UML can be used very efficiently to design the model of E-Commerce system [17, 18].

UML consists of a number of graphical elements that may be combined to form a diagram. The purpose of the diagram is to present multiple views of a system, and this set of multiple views is called a model. UML model describes what a system is supposed to do. It doesn't tell how to implement the system. UML includes nine diagrams namely Class diagram, Object diagram, Use Case diagram, Sequence diagram, Collaboration diagram, Statechart diagram, Activity diagram, Component diagram, and Deployment diagram which help to design a system.

To model our proposed system we only consider the Use Case diagram, Sequence diagram and also the Collaboration diagram [c.f. Appendix-A]. Use Cases are used to document the proposed system requirements and provides a useful technique which helps us to clarify exactly what the system is supposed to do.

4. Methodology

4.1 Identification of Objects

The objects that require in designing the proposed payment system in E-Commerce are described below:

Customer: Holder of a payment card, such as a credit card or debit card from an Issuer.

Issuer: A financial institution, such as a bank, that provides the customer a payment card and is responsible for the cardholder’s debt payment.

Merchant: Merchant is the person or organization sells goods or services to the cardholder through web and has an account in the Acquirer.

Acquirer: A financial institution which processes payment card authorizations and makes payments. The Acquirer provides electronic transfer of funds to the Merchant’s account from the Customer’s account through Issuer over a secured payment network.

4.2 Use Cases

Given the above objects we propose the newly developed model, subdivide into a number of Use Cases. Here each Use Cases denotes a subsystem.

4.2.1 Use Case 1: Customer

As in Figure 1 there are six different use cases related to the Customer activity into the system, these are

- o Browse/select items: Browse and select items from the Merchant Web site
- o Make order: Make an order of those selected item
- o Collect order & Merchant info: Collect placed order information and Merchant information from the Merchant
- o Send order & Merchant info: Send collected information from the Merchant to the Issuer
- o Cancel order: Cancel selected or all already ordered items
- o Make payment: Make payment to the Merchant through the Issuer

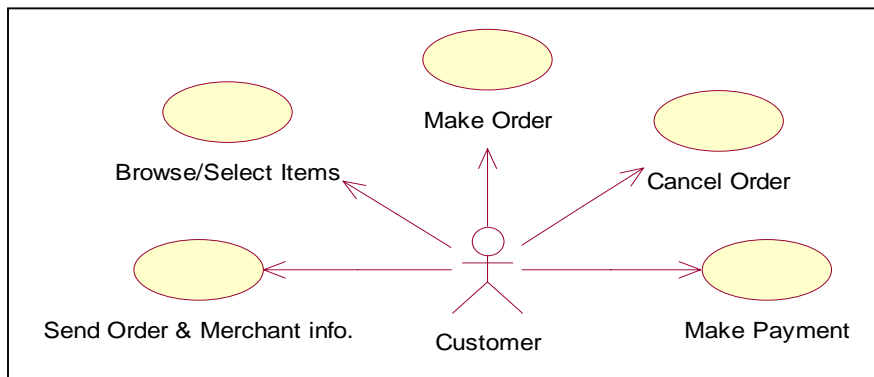


Figure 1: Use Case 1

4.2.2 Use Case 2: Merchant

As in Figure 2 there are seven different use cases related to the Merchant activity in the system, these are

- Place Item on the Web: Place products/items on the web for possible purchase by the Customer
- Process order: Process all order placed by the Customer
- Send order info: Send the placed order information to the Customer. This use case extends the Process Order use case
- Collect DRM package: Collects DRM package from the Issuer
- Send DRM package: Send the DRM package to the Acquirer, this is an extended use case of the Collect DRM Package
- Confirm order: Confirm order to the Customer
- Collect payment: Collect payment from the Acquirer

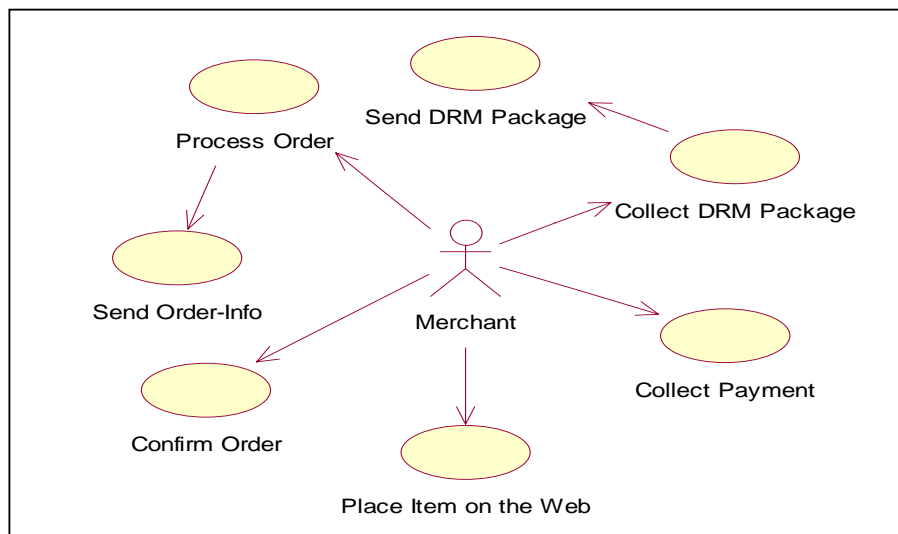


Figure 3: Use Case 2

4.2.3 Use Case 3: Issuer

As in Figure 3 there are nine different use cases related to the activity performed by the Issuer in the system, these are

- Collect order info: Collect information about the order placed by the Customer
- Validate Customer: Verify and validate the customer information
- Generate token: Process the submitted order and generate a single use 'token'
- Create DRM package: Create the DRM package by wrapping the 'token' along with it's usage rights
- Send DRM package: Send the DRM package to the Merchant
- Collect token: Collect unwrap 'token' from the Acquirer
- Validate token: Validate the 'token'
- Transfer fund: Transfer fund from the Customer account to the Merchant account
- Confirm fund transfer: Confirm the Customer about the fund transfer.

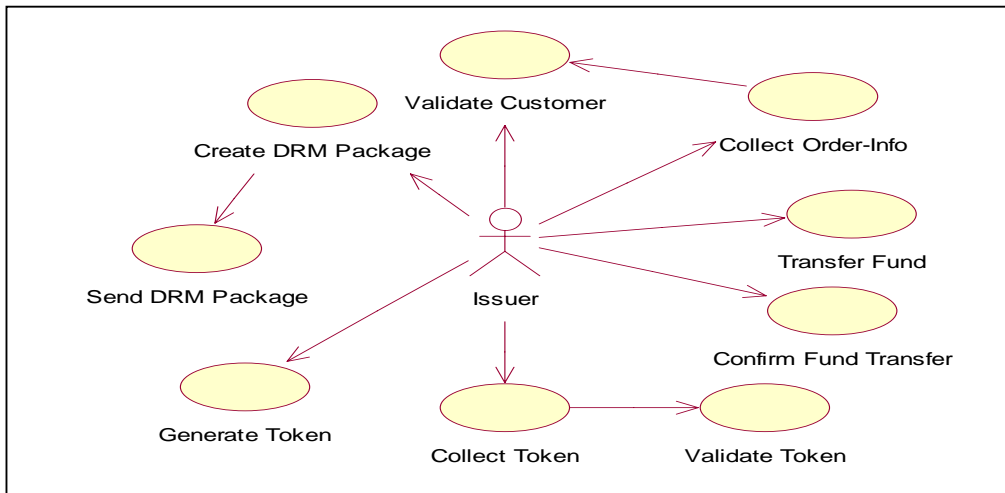


Figure 3: Use Case 3

4.2.4 Use Case 4: Acquirer

As in Figure 4 there are seven different use cases, these are

- o Collect DRM package: Collect DRM package from the Merchant
- o Validate Merchant: Validate the authenticity of the Merchant
- o Unwrap DRM package: Process the DRM package and unwrap it
- o Find Token: Collect the 'token' from the unwrapped DRM package
- o Send Token: Send the 'token' to the Issuer for the payment
- o Transfer Fund: Transfer fund from the Customer's account to the Merchant's account through the Issuer
- o Send Fund transfer conformation: Confirm fund transfer to the Merchant.

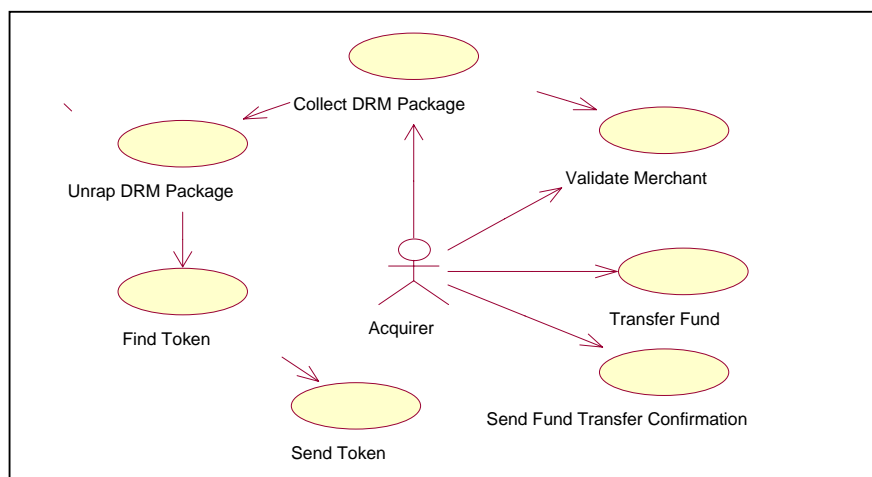


Figure 4: Use Case 4

4.3 The Sequence Diagram

The Sequence Diagram which describes the time dependent communication through message passing between the objects is illustrated below. Figure 5 describes how the Customer, Merchant, Issuer and the Acquirer are communicating with each other.

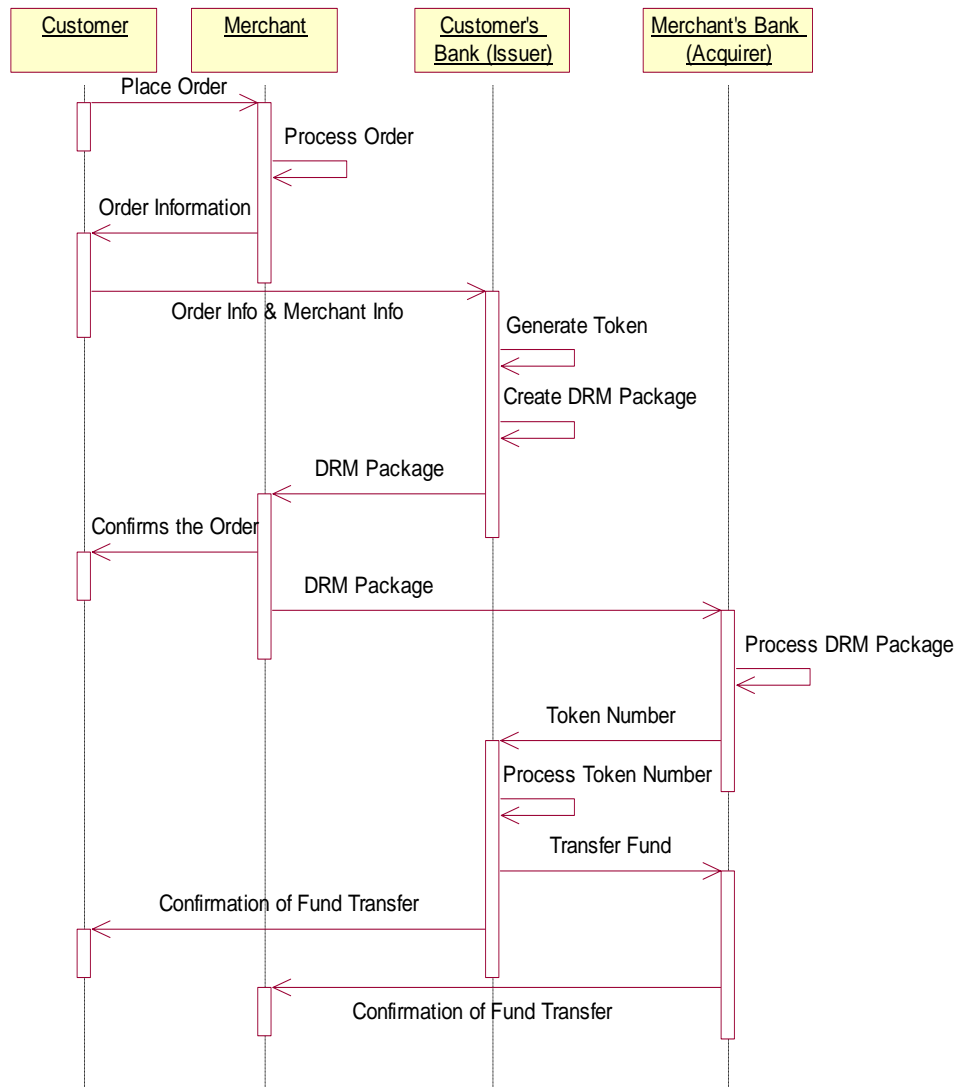


Figure 5: Sequence Diagram of the Secure Credit Card Payment System

It is assumed that the customer rely only the bank or the Credit Card Agency (CCA) over the web to disclose his/her identity [12]. To purchase a product or service the customers can involve their banks on their behalf. Therefore, the customers need not give their respective credit card numbers to the merchants, and can feel safe. The merchant send the order information to the customer and the customer is to redirect all the information to the bank. On behalf of the customer, the rest of the transaction is to be handled by the bank. In order to perform this, bank will be required to issue a *token* that will expire after a single use or after a time limit. The *token* is basically a 'wrapped DRM package' of the numbers and the rights to use them. This number is totally different from the customer's credit card number. The right includes different Intellectual Property (IP) such as, the purchase amount, category of product purchased [such as books, household, cloth etc.], merchant's name, date of issue, date of expiry, customer name etc. The merchant will then redirect the *token* to his/her bank. On having the *token* the merchant's bank will *unwrap the package*, collect the *token* and the necessary information needed to process the transaction and will transfer the amount from the customer's bank.

The advantages of our proposed system are as follows:

- The *token* will be generated using the information order provided by the customer and about the merchants. This would ensure that only the specified merchant can use the *token*.
- Along with merchant information the *token* will also wrap the customer information.
- The package can be unwrapped only by using a specific application [such as Adobe Acrobat], that will take care of the rights imposed on the package and will restrict its use.
- Minimization or even no interaction of the third party vendors [such as VeriSign, PayPal etc] in payment transaction process is possible.
- In the whole process of transaction the customer will never disclose his/her credit card number. This will ensure trust in the minds of the customer and this will encourages them to take part in E-Commerce transaction.

5. Conclusion

Lots of efforts have been made to ensure trust to the participated customers in the E-Commerce transaction system. Several considerations have been made in order to provide security to the participants of such system. However, no such efficient functional solution to fill the observed deficiency of the E-Commerce transaction system has so far even developed.

In our paper an attempt has been made to throw some light on the different risks and also to offer a solution to fill such deficiency of the system of E-Commerce. In order to do this we first consider the participants related to our system, followed by a sketch identifying the association and interaction of such participants under the proposed system.

The proposed model can be successfully applied by means of making a very little change in the current E-Commerce transaction system. In future this proposed model may also be utilized for the purpose of managing information securely in the M-Commerce transaction system.

References:

- [1]. "The Technology of Rights: Digital Rights Management", Karen Coyle, Based on a talk originally given at the Library of Congress, November 19, 2003
- [2]. "E-Commerce – An Indian Perspective", P.T.Joseph, S.J, PHI, 2nd Edn, 2006
- [3]. <http://www.epaynews.com>
- [4]. <http://www.nasscom.org>
- [5]. "Cryptography and E-Commerce", Jon C.Graff, Wiley, ISBN: 0471-40574-4, 2001
- [6]. "E-Commerce and E-Business: Rising from the Ashes", T.Pritsky, Whitepaper, www.hill.com, Dec 2002.
- [7]. Netscape Website: <http://www.netscape.com/newsref/std/SSL.html>
- [8]. MasterCard Website: <http://www.mastercard.com>
- [9]. "Building an E-Commerce Trust Infrastructure SSL Server Certificates and Online Payment Services", VeriSign Technical Brief, www.verisign.com
- [10]. http://www.setco.org/download/set_bk1.pdf
- [11]. "Off-line generation of limited-use credit card numbers", Aviel D. Rubin, Rebecca N.Wright, Financial Cryptography Conference, Feb 2001
- [12]. "A Survey of Security in Online Credit Card Payments", Umesh Shankar, Miriam Walker, May 2001
- [13]. American Express website: <http://www26.americanexpress.com>
- [14]. T.Huang, Y.Liu, "Considerations on AVS DRM Architecture", Jour. of Computer Science and Technology, Vol. 21, No. 3, DOI. 10.1007/s11390-006-0366-4, May, 2006
- [15]. P.Koster, F.Kamperman, P.Lenoir, K.Vrieling, "Identity-Based DRM: Personal Entertainment

Domain”, LNCS, Vol. 4300, DOI. 10.1007/11926214_4, 2006

[16]. H.Kim, Y.Lee, B.Chung, H.Yoon, J.Lee, K.Jung, “Digital Rights Management with Right Delegation for Home Networks”, LNCS, Vol. 4296, DOI. 10.1007/11927587_20, 2006

[17]. J. Nutzel, A.Beyer, “How to Increase the Security of Digital Rights Management Systems Without Affecting Consumer’s Security”, LNCS, Vol. 3995, DOI. 10.1007/11766155_26, 2006

[18]. M.Petkovic, R.P.Koster, “User Attributed Rights in DRM”, LNCS, Vol. 3919, DOI. 10.1007/11787952_6, 2006

[19]. B.Vassiliadis, V.Fotopoulos, A.N.Skodras, “Decentralising the Digital Rights Management Value Chain by means of Distributed License Catalogues”, LNCS, Vol. 204, DOI. 10.1007/0-387-34224_9_81, 2006

[20]. B.B.Zhu, Y.Yang, T.Chen, “A DRM System Supporting What You See Is What You Pay”, LNCS, Vol. 3919, DOI. 10.1007/11787952_26, 2006

[21]. R.Iannella, “Digital Rights Management (DRM) Architectures”, D-Lib Magazine, Vol. 7, No. 6, ISSN 1082-9873, June 2001.

[22]. G.Booch, J.Rumbaugh, I.Jacobson, “Unified Modeling Language User Guide”, Addison Wesley, 2nd Edition, ISBN: 0- 321-26797-4, 2005.

[23]. P.Kruchten, “The Rational Unified Process”, Addison-Wesley Longman Inc, 3rd Edition, 2004.

[24]. IBM’s Rational Rose: (<http://www.rational.com>).

[25]. S.Banerjee, S.Karforma, S.Ghosh, “A DRM Based Credit Card Transaction in E-Commerce System”, 41st National Convention of CSI, November 23-25, 2006, Tata McGraw-Hill, ISBN-0-07-062171-3, pp-107-110, 2006.

[26]. K.Lee, D.E.Booth, “A Prototype System Developed for Digital Rights Management in Electronic Commerce”, Jour. of Internet Commerce, Vol. 3, No. 4, pp. 93-117, ISSN 1533-2861, 2004.

[27]. S. Banerjee, D. E. Booth, S. Ghosh, S. Mukhopadhyay, “A Prototype Design for Digital Intellectual Property Right Management in E-Commerce - A UML Based Approach”, Journal of the Computer Society of India, Vol 36 No 4 (Oct-Dec 2006), pp-46-51, ISSN-0254-7813, 2006.

Appendix-A (Collaboration Diagram)

