DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4567

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

E-COMMERCE SECURITY WITH SECURE ELECTRONIC TRANSACTION PROTOCOL : A SURVEY AND IMPLEMENTATION

Prof. Prathamesh Churi
Department of Computer Engineering
SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering
Mumbai, India

Abstract: This paper presents review about transaction processing on ecommerce website using Secure Electronic Transaction (SET) protocol. SET is a very comprehensive security protocol, which utilizes cryptography to provide confidentiality of information, ensure payment integrity, and enable identity authentication. It relies on cryptography, digital certificate and authentication by SMS to ensure message confidentiality and security. First the report introduces about ecommerce websites and how to build it. It then explains how SET works and the components involved in it. Then the report gives out a design and implementation of this protocol.

Keywords: SET; E-Commerce; SSL; Security.

I. INTRODUCTION

E Commerce stands for electronic commerce and caters to trading in goods and services through the electronic medium such as internet, mobile or any other computer network [1,2,3]. With the growing use of internet worldwide, Electronic Data Interchange (EDI) has also increased in humungous amounts and so has flourished ecommerce with the prolific virtual internet bazaar inside the digital world which is righty termed as e-malls [17 18 19 20]

With e-commerce then, you can buy almost anything you wish for without actually touching the product physically and inquiring the salesman n number of times before placing the final order. Here is a beautiful picture depicting how has human life evolved to adapt to the digital world and hence trading over the internet.

Most of online purchases are paid for by a credit card. Merchants like credit card payments because an instant authorization guarantees that the card is valid (as opposed to a check which may bounce). Customers like paying by credit cards because they can easily cancel a transaction in case when they don't receive products or services according to the agreement in the transaction. While some of credit card payments for online services are performed by phone, most of such payments are made by filling in an online form.

Credit card information submitted by the customer is sent to the bank which has issued the credit card to verify. If the transaction is approved, the merchant notifies the customer that the order has been placed. The actual transfer of money from the credit card bank to the merchant may happen in a few hours, or even in a few days.

Merchants who accept credit card payments pay fee (between 1 and 7 percent of the card charge) for each card charge. In addition, in some cases merchants pay authorization fee for each credit card authorization attempt, as well as other fees related to credit card processing.

This massive increase in the uptake of ecommerce has led to a new generation of associated security threats, but any ecommerce system must meet four integral requirements i.e. privacy, integrity, authentication and nonrepudiation [21 22 23 24 25]. A protocol designed to ensure the security and integrity of online communications and purchases, Secure Electronic Transaction (SET) uses digital certificates, issued to merchants and other businesses and customers, to perform a series of security checks verifying that the identity of a customer or sender of information is valid. SET provides the basic framework within which many of the various components of securing digital transactions function. Digital certificates, digital signatures, and digital wallets all function according to the SET protocol.

A. SET Protocol [4,5,6,7, 33]

Electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce. Even though SSL is extremely effective and widely accepted as the online payment standard, it requires the customer and merchant to trust each other. An undesirable requirement even in face-to face transactions, and across the Internet it admits unacceptable risks.

MasterCard and VISA developed SET in collaboration from leading technology companies, which includes Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems and VeriSign. On February 1st 1996 these companies announced the single technical standard for safeguarding the payment purchases made over open networks. This standard is called as the SET Secure Electronic Transaction specification. SET specification includes, digital certificates, which is a verifying the actual identity of the parties participating in the transaction. By using these sophisticated cryptographic techniques, SET protocol, aims to make cyberspace a safer place for conducting business and thereby increase consumer confidence in E-Commerce.

SET was developed to address these major requirements in the online shopping industry: [8]

- Provide confidentiality of information -- accomplished by the use of message encryption
- Ensure the integrity of all transmitted data – accomplished by the use of digital signatures
- Authenticate a cardholder meaning that he is the legitimate user of the branded payment card – accomplished by the use of digital signatures and cardholder certificates

- Authenticate a merchant to accept payment card transactions and assure his relationship with an acquiring financial institution – accomplished by the use of digital signatures and merchant certificates
- Protect all legitimate parties involved in the transaction using the best security practices
- Facilitate interoperability among software and network providers – accomplished by the use of specific protocols and message formats.

B. Problem with SSL. [9,10,11]

The SSL protocol, widely deployed today on the Internet, has helped create a basic level of security sufficient for some hearty souls to begin conducting business over the Web. SSL is implemented in most major Web browsers used by consumers, as well as in merchant server software, which supports the seller's virtual storefront in cyberspace. Hundreds of millions of dollars are already changing hands when cybershoppers enter their credit card numbers on Web pages secured with SSL technology[26 27 28]. In this sense, SSL provides a secure channel to between the consumer and the merchant for exchanging payment information. This means any data sent through this channel is encrypted, so that no one other than these two parties will be able to read it. In other words, SSL can give us confidential communications, it also introduces huge risks:

- The cardholder is protected from eavesdroppers but not from the merchant. Some merchants are dishonest: pornographers have charged more than advertised price, expecting their customers to be too embarrassed to complain. Some others are just hackers who put up a snazzy illegal Web site and profess to be the XYZ Corp., or impersonate the XYZ Corp. and collecting credit card numbers for personal use.
- The merchant has not protected from dishonest customers who supply an invalid credit card number or who claim a refund from their bank without cause. Contrary to popular belief, it is not the cardholder but the merchant who has the most to lose from fraud. Legislation in most countries protects the consumer.

C. SET Protocol Components [12]:

What we want here is a protocol very similar to credit card transactions at a local store, something SSL doesn't mimic in functionality. SET is the one.

The purpose of the SET protocol is to establish payment transactions that

- Provide confidentiality of information.
- Ensure the integrity of payment instructions for goods and services order data.
- Authenticate both the cardholder and the merchant.

There are four main entities in SET:

- Cardholder (customer)
- Merchant (web server)
- Merchant's Bank (payment gateway, acquirer): payment gateway is a device operated by an acquirer. Sometime, separate these two entities. Issuer (cardholder's bank)

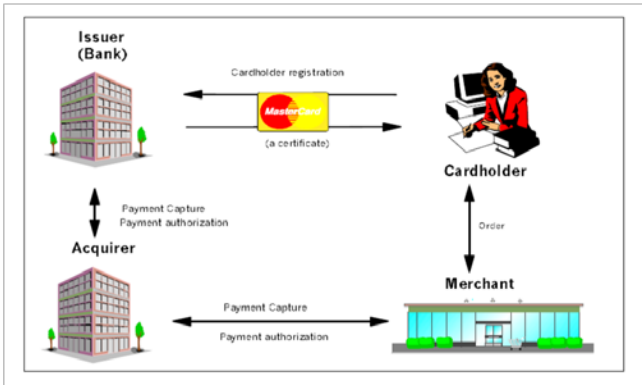

Figure 1. SET Protocol Components .

II. REQUIREMENT ANALYSIS AND LITERATURE SURVEY

In electronic commerce at least two sets of parties (with broadly similar interests within each set) will need to participate: customers and merchants on the one hand, and financial institutions and regulators on the other hand. Arbitrators may be needed in case of a dispute.

A. Concerns of customers and merchants

Customers and merchants will have an almost common set of wishes and concerns for electronic commerce mechanisms:

- **Security [13]:** Electronic currency is just data and is easily copied. It has to be assured that no-one else can divert a payment or impersonate another person in order to steal his funds. Moreover, every party should be protected from a collusion of other parties (multi-party security). No party in the system needs to trust another party - or at least the trust should be as little as possible – to ensure his security. The acclaimed security properties must be publicly verifiable.
- **Acceptability [15]:** A wide range of parties needs to accept the payment.
- **Convenience [16]:** To make small purchases, the actions required during a transaction should be minimal. This pertains not only the physical efforts required of a party, but also the speed by which the transaction is processed. This includes: speed, reliability, fungible (the 'currency' or payment unit should be divisible), transferability (peer-to-peer payments) and minimal specific hardware.
- **Cost [28]:** Preferable no additional cost, hence no effective lower limit to the value of a transaction. Transaction costs include any direct costs, at the customer, merchant and at any intermediary, as well as processing or handling time for all parties.
- **Privacy [29]:** Today, cash is a more or less anonymous payment mechanism. No external party (individual, company or other authority) can create a historic record of any individual's cash transactions. With electronic money the bank, or any other party should not be able to determine whether two payments were made by the same user.
- **Durability [30]:** The electronic money should not be easily 'lost'. For example, when a system crashes.

B. Requirements for financial institutions:

The financial institutions that will provide services to enable these transactions in the market space, and regulators will also have a set of requirements for a payment mechanism:

- Immediate control: Financial institutions and regulators will seek a system in which transactions are controlled or cleared individually, so that any breach of security can be identified as soon as possible.
- Traceability: Financial institutions and regulators will seek a system in which transactions are traceable, so that if a crime is detected the culprit can be identified. In particular, traceability will be important to track international funds flows, tax evasion and money laundering.
- Control over the spread of encryption mechanisms: A key concern of the government, and therefore any regulatory body, is to control the spread of encryption mechanisms.

C. *Merchant certificates [31 32]:*

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window—the decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand. Because they are digitally signed by the merchant's financial institution, merchant certificates cannot be altered by a third party and can only be generated by a financial institution. These certificates are approved by the acquiring financial

Institution and provide assurance that the merchant holds a valid agreement with an Acquirer. A merchant must have at least one pair of certificates to participate in the SET environment, but there may be multiple certificate pairs per merchant. A merchant will have a pair of certificates for each payment card brand that it accepts.

D. *Existing Ecommerce Protocols and Security Feature Comparison*

Table I : Security Feature Comparison

Feature /Protocol	Proposed work	[34]	[35]	[36]	[37]	[38]	[39]
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non – repudiation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Forward Secrecy	NR	NR	NR	NR	NR	NR	NR
Order Secrecy	NR	NR	NR	NR	NR	Yes	Yes
Payment Secrecy	Yes	Yes	Yes	Yes	Yes	NR	NR

III. METHODOLOGY

A. *Block Diagram of proposed work :*

In a SET implementation, the merchant customizes order forms to allow shoppers to request the payment initiation message, also known as the wakeup message, from a merchant server. When the shopper's Web browser receives this payment initiation message shoppers specify payment card information. After inserting payment card information browser launches authentication mechanism for cardholder.

A verification code is send to cardholder's mobile. Unless and until that code is being inserted the order is not get placed. By inserting verification code the cardholder is authenticated and order is placed after submitting the code. When the form is submitted, the credit card information is encrypted using SSL. It is then passed to the acquirer, using regular SET messages, through the Payment Gateway.

Since the SET protocol starts from the merchant server, you need to change the way to process the transactions and APIs compared to the process with a wallet.. The process is explained in the list that follows.

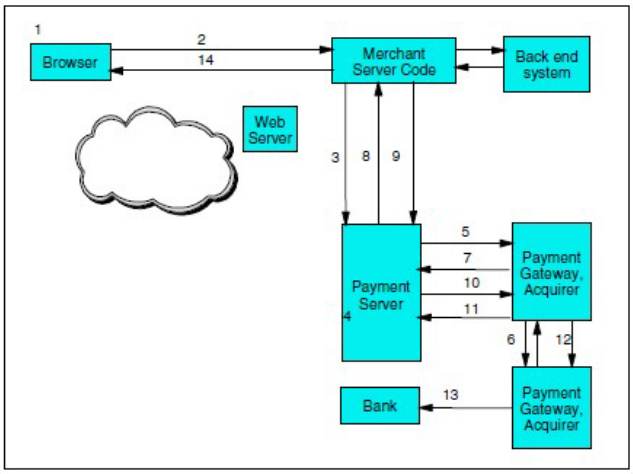

Figure 2. SET Protocol Components

B. *Steps of proposed Work*

- A cardholder decides to make a purchase.
- When the cardholder clicks the Buy button, a command is sent to the merchant server.
- The merchant server calls the Payment Server etAcceptPayment() API.
- The Payment Server checks to see if authorization should be done at this point. For example, if the merchant's acquirer is available.
- When authorization can be done, the server generates an Authorization Request (AuthReq) sends it to the acquirer,s and waits for an Authorization Response message (AuthRes).
- The acquirer software or Payment Gateway receives the request. Using a normal back-end network or other communication channels, the acquiring institution contacts the cardholder's issuing institution. It checks that the payment card is valid and that the cardholder has sufficient funds or credit to make the purchase.
- The AuthRes message is received by the Payment Server and processed. Information is stored in the database for record-keeping and further order processing.
- The merchant can now fulfill the order.
- When the goods are shipped, the merchant requests payment by calling the etDeposit() API.
- The Payment Server now begins the capture process by sending a Capture Request to the Payment Gateway. Capture is the transfer of funds from the merchant's acquirer to merchant and onward to merchant's acquirer from cardholder's issuing institution.
- The payment gateway receives the capture request and sends it a capture response message.
- The payment gateway uses the closed (back-end) network to contact the merchant's acquirer and requests the transfer of payment. The acquirer deposits the payment to the merchant's account.

- The merchant server sends the confirmation to the cardholder.
- The cardholder's issuing bank deposits the payment to the merchant's bank account and updates cardholder's account in cardholder's issuing bank.

IV. RESULTS AND ANALYSIS

In this section , privacy aspect of SET protocol is compared with MSET . In addition , analytical evaluation for SET Vs MSET will be introduced.

Table II shows the comparison between SET and MSET protocols . from privacy protection perspectives.

Table II : Privacy Protection Comparison between SET and MSET

Parameters	SET	MSET
Anonymity	No	No
Pseudonymity	No	Yes
Unlinkability	No	Yes
Identity Protection From Payee [34 , 35]	No	Yes
Identity Protection From Eavesdropper [34 , 35]	Yes	Yes
Transaction Privacy Protection From Eavesdropper. [34 , 35]	Yes	Yes
Transaction Privacy Protection From TTP or Related Financial Institution [34 , 35]	No	Yes

To obtain representative performance evaluation results, the average execution time of encryption, decryption and hash function application are calculated for 1000 instances on a Personal machine with specifications "Intel Core i3 with 2.13 Ghz processor and 4.00 GB RAM". The outcome is illustrated in Table III. We choose for symmetric encryption the AES algorithm with key size 256, for asymmetric encryption the RSA algorithm with key size 1024, and SHA algorithm with 256 key size for hashing all with message size 100 bit. Such values were used to achieve higher security levels with a relatively low number of computations without affecting performance.

Table III : Opeartion Exceution Time in SET Protocol

Operation	Algorithm	Key Size	Message Size	Execution Time
Symmetric Encryption	AES	256	100 bit	16.5
Symmetric Decryption	AES	256	100 bit	16.5
Asymmetric Encryption	RSA	1024	100 bit	16.5
Asymmetric Decryption	RSA	1024	100 bit	37.2
Hash	SHA 256	-	100 bit	556.5

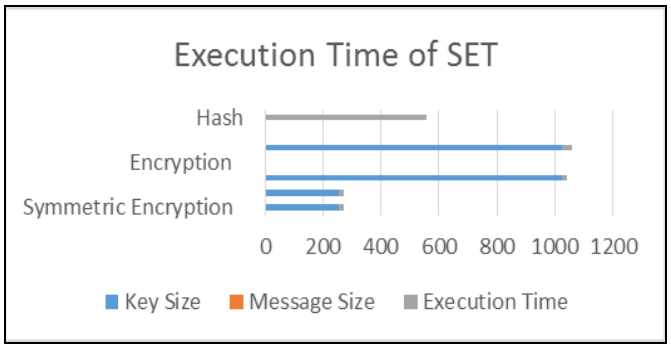

Figure 3. Execution Time of SET Protocol

V. CONCLUSION

The SET protocol which was introduced theoretically way back but was not widely used due to its disadvantages such as the customer has to download a software for using SET protocol for customer authentication which was not desirable and the protocol deals with digital certificates and strong encryption technologies which makes the system complex to use and process.

The aim was to implement SET protocol by removing its disadvantages and adding an equivalent functionality to achieve a better security feature was successfully implemented. The customer authentication was achieved by sending a verification code to the customer's mobile phone and website authentication was achieved providing a Standard SSL certificate for the website. The project is supported by strong cryptographic techniques to store the customer's confidential data as encrypted data and password are stored in hashed form.

VI. ACKNOWLEDGMENT

I want to thank my brother Mr. Rohan Chaudhari for his encouragement in this research work.

VII. REFERENCES

[1] X. Zhang, Q. Huang and P. Peng, "Implementation of a Suggested E-commerce Model Based on SET Protocol," *2010 Eighth ACIS International Conference on Software Engineering Research, Management and Applications*, Montreal, QC, Canada, 2010, pp. 67-73.

[2] A. Sun, "Optimization Study for Lightweight Set Protocol," 2012 International Conference on Industrial Control and Electronics Engineering, Xi'an, 2012, pp. 1206-1209.

[3] X. Liu, "The Study on E-commerce Security Based on ECC and SET," *2011 Third International Conference on Communications and Mobile Computing*, Qingdao, 2011, pp. 85-87.

[4] X. Fei, A. M. Zhang and W. Liang, "Formalizing and Checking SET Protocol Based on TLA," *2010 International Conference on E-Product E-Service and E-Entertainment*, Henan, 2010, pp. 1-3.

[5] S. p. Chen, "Study on a Safe and Efficient Payment Model in E-Commerce," *2008 International Conference on Advanced Computer Theory and Engineering*, Phuket, 2008, pp. 860-864.

[6] X. Zhang and L. Wang, "Key Technologies for Security Enhancing of Payment Gateway," *2008 International Symposium on Electronic Commerce and Security*, Guangzhou City, 2008, pp. 743-748.

[7] M. C. Ruiz, D. Cazorla, F. Cuartero and J. J. Pardo, "A formal specification and performance evaluation of the purchase phase in the SET protocol," *Seventh International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'05)*, 2005, pp. 6 pp.-.

[8] Seokwon Yang, S. Y. W. Su and H. Lam, "A non-repudiation message transfer protocol for e-commerce," *EEE International Conference on E-Commerce, 2003. CEC 2003.*, 2003, pp. 320-327.

[9] G. Bella, F. Massacci and L. C. Paulson, "Verifying the SET registration protocols," in *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 1, pp. 77-87, Jan 2003.

[10] M. Papa, O. Bremer, J. Hale and S. Shenoi, "Formal analysis of e-commerce protocols," *Proceedings 5th International Symposium on Autonomous Decentralized Systems*, Dallas, TX, 2001, pp. 19-28.

[11] Z. Hu, "The Study of E-Commerce Security Protocol," *2011 International Conference on Intelligence Science and Information Engineering*, Wuhan, 2011, pp. 349-352.

[12] Shen zihao and Wang hui, "An improved SET protocol payment system," *2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*, Chengdu, 2010, pp. 400-403.

[13] B. Xu and S. Xie, "Research of Session Security Management in E-Commerce System," *2009 International Symposium on Information Engineering and Electronic Commerce*, Ternopil, 2009, pp. 796-799.

[14] Z. Zhang, "E-Commerce Based Agents over P2P Network," *2008 International Conference on Management of e-Commerce and e-Government*, Jiangxi, 2008, pp. 77-81.

[15] Chin-Ming Hsu and Hui-Mei Chao, "An online fraud-resistant technology for credit card E-transactions," TENCON 2007 - 2007 IEEE Region 10 Conference, Taipei, 2007, pp. 1-4.

[16] P. Venkataram, B. S. Babu, M. K. Naveen and G. H. S. Gungal, "A Method of Fraud & Intrusion Detection for E-payment Systems in Mobile e-Commerce," *2007 IEEE International Performance, Computing, and Communications Conference*, New Orleans, LA, 2007, pp. 395-401.

[17] Hyun-Seok Kim, Il-Gon Kim and Jin-Young Choi, "Analyzing the Application of E-Commerce inWireless Network," *Second IEEE International Workshop on Mobile Commerce and Services*, Munich, 2005, pp. 112-122.

[18] H. Schuldt, A. Popovici and H. J. Schek, "Automatic generation of reliable e-commerce payment processes," *Proceedings of the First International Conference on Web Information Systems Engineering*, Hong Kong, 2000, pp. 434-441 vol.1.

[19] Ramkrishna Oruganti, Saurabh Shah, Yohan Pavri, Neelansh Prasad, Prathamesh Churi (2017). JSSecure: A Secured Encryption Strategy for Payment Gateways in E-Commerce. Circulation in Computer Science, 2, 5(June 2017), 13-17.

[20] Meadows, Catherine, and Paul Syverson. "A formal specification of requirements for payment transactions in the SET protocol." In *International Conference on Financial Cryptography*, pp. 122-140. Springer, Berlin, Heidelberg, 1998.

[21] Lu, Shiyong, and Scott A. Smolka. "Model checking the secure electronic transaction (SET) protocol." In *Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999. Proceedings. 7th International Symposium on*, pp. 358-364. IEEE, 1999.

[22] Brlek, Srecko, Sardaouna Hamadou, and John Mullins. "A flaw in the electronic commerce protocol SET." *Information Processing Letters* 97, no. 3 (2006): 104-108.

[23] Shedid, Sabrina M., and Mohamed Kouta. "Modified SET protocol for mobile payment: an empirical analysis." In *Software Technology and Engineering (ICSTE), 2010 2nd International Conference on*, vol. 1, pp. V1-350. IEEE, 2010.

[24] Paulson, Lawrence C. "Verifying the SET protocol: Overview." In *Formal Aspects of Security*, pp. 4-14. Springer, Berlin, Heidelberg, 2003.

[25] Seo, Moonseog, and Kwangjo Kim. "Electronic funds transfer protocol using domain-verifiable signcryption scheme." In *ICISC*, vol. 99, pp. 269-277. 1999.

[26] Seo, Moonseog, and Kwangjo Kim. "Electronic funds transfer protocol using domain-verifiable signcryption scheme." In *ICISC*, vol. 99, pp. 269-277. 1999.

[27] Kraft, Theresa A., and Ratika Kakar. "E-commerce security." In *Proceedings of the Conference on Information Systems Applied Research, Washington DC, USA*. 2009.

[28] Marchany, Randy C., and Joseph G. Tront. "E-commerce security issues." In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pp. 2500-2508. IEEE, 2002.

[29] Udo, Godwin J. "Privacy and security concerns as major barriers for e-commerce: a survey study." *Information Management & Computer Security* 9, no. 4 (2001): 165-174.

[30] Marchany, Randy C., and Joseph G. Tront. "E-commerce security issues." In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pp. 2500-2508. IEEE, 2002.

[31] Kesh, Someswar, Sam Ramanujan, and Sridhar Nerur. "A framework for analyzing e-commerce security." *Information Management & Computer Security* 10, no. 4 (2002): 149-158.

[32] Laudon, Kenneth C., and Carol Guercio Traver. *E-commerce*. Pearson, 2013.

[33] Sengupta, A., C. Mazumdar, and M. S. Barik. "e-Commerce security—A life cycle approach." *Sadhana* 30, no. 2 (2005): 119-140.

[34] Mastercard and Visa. SET Protocol Specifications. http://www.setco.org/set_specifications.html

[35] Romao A. and da Silva M. M., 1998. An Agent-based Secure Internet Payment Systems. Proceedings of TREC'98, LNCS 1402, pp. 80-93.

[36] Wang X. F. et al, 1999, "Secure Agent-Mediated Mobile Payment" Proceedings of PRIMA98, LNAI 1599, pp.162- 173.

[37] Supakorn Kungpisdan , Bala Srinivasan , Phu Dung Le, "A Practical Framework for Mobile SET Payment" In Proceedings of the IADIS International E-Society Conference, Lisbon, Portugal, June 3-6 (2003) , pp 321-328

[38] Chung-Ming Ou, C.R.Ou, "SETNR/A: an agent-based secure payment protocol for mobile commerce", International Journal of Intelligent Information and Database Systems, Vol. 4, No.3, 2010.

[39] Xiaolin Pang, Kian–Lee Tan, Yan Wang, and Jian Ren, "A Secure Agent-Mediated Payment Protocol", In: Fourth International Conference on Information and Communications Security (ICICS2002), volume LNCS 2512, Springer-Verlag, pages 422-433

