

## Enhanced E-Business Layered Architecture (secured contact)

د. ندى ماجد الحكاك\*

م. نوال علاء الدين الجراح\*\*

### الملخص

إن أحد العوامل التي تؤثر على نجاح عمل الشركات والأفراد هو استخدام هيكلية مرنة وأمنة للأعمال الإلكترونية المرتبطة ببيئة عملهم الإلكتروني ، لأن الأعمال الإلكترونية تؤثر على كفاءة الخدمة المقدمة للبائع والمشتري. بشكل عام توجد دراسات عديدة أجريت في هذا المجال بهدف تحسين البنية التحتية للأعمال الإلكترونية من خلال تقسيم العمل فيها إلى عدة مستويات أو طبقات . وبالرغم من هذا فإنها مازالت تعاني من عدة محدوديات عند تطبيقها في العالم الخارجي. هذا البحث يهدف إلى تقديم هيكلية طبقية للأعمال الإلكترونية تهدف إلى محاكاة الواقع العملي للسوق وبشكل أكثر مرونة إضافة إلى التركيز على جانب الحماية، بالنسبة للتعاملات ما بين التاجر والمستهلك في بيئة الإنترنت. حيث تم اقتراح خوارزمية CTAM لتأمين محادثة سرية ما بين طرفين عبر شبكة الإنترنت الغير آمنة.

### Abstract

Defining a practical e-business infrastructure is an important issue for all parties who deal with electronic environment because e-business affects the quality of services presented for sellers and buyers. Many works have been done trying to enhance the e-business infrastructure by splitting its work into levels or layers, yet most of those models had many limitations in the real world.

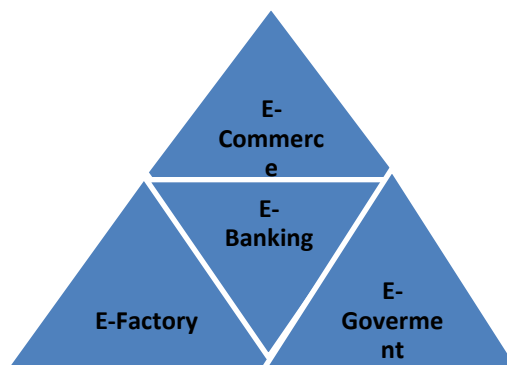
This paper presented a new enhanced e-business layered architecture with constraint on presenting a secured communication over the internet between the customer and merchant. By using CTAM algorithm, the proposed algorithm is more secure and flexible than original security algorithm.

**Keywords:** Customer Trusted Arbitrator Merchant (CTAM)

### Introduction

E-business is a method of achieving marketing objectives by using electronic communication technology. While Marketing is the management process with multiple responsibilities like: identifying, anticipating, and satisfying customer requirements profitability (Chaffey, 2004). Generally, E-business contains multiple electronic processes as in figure (1).

\* قسم علوم الحاسبات - كلية بغداد للعلوم الاقتصادية الجامعة  
\*\* كلية الإدارة والاقتصاد - الجامعة المستنصرية



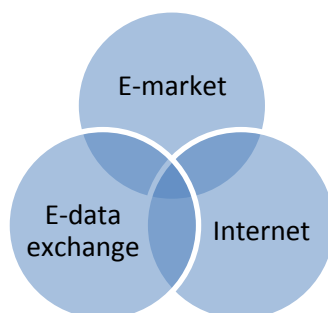
**Figure (1): E-business and E-commerce**

E-commerce represents one of the main aspects for "Digital Economy", because digital economy deals with two main aspects; e.g. e-commerce and Information Technology (IT). Information Technology created the meaning of e-commerce as it depends on many items, like: computing, communication, and different activities to deal with marketing area (Havyatt, 2011).

E-commerce styles are; e.g.; review of goods and services over the internet, buying things depending on their descriptions, electronic payment over the network. However, E-commerce factors are; privacy, computer crimes, intellectual property, electronic payment, security factors, taxes (Santti, 2011). Moreover, E-commerce activities represented as transactions between two parties like: Business-to-Business (B2B) where the transactions are between two organizations, Business-to-Consumer where the transactions are between an organization and consumers (B2C), Consumer-to-Business (C2B), Consumer-to-Consumer (C2C) (Chong, 2011) and (Chaffey, 2004).

Furthermore, E-commerce benefits are: more active marketing with higher profits, decrease time and efforts, customer is free to select any choice between multiple choices; customers can buy with cost prices, higher satisfactions of customers (Montgomery, 2009). On the other hand e-commerce have some limitations; e.g. parties may be unserious in information's exchange, delay delivery, the delivered product may not match the requested one, delay duplicity lows (Lau, 2005).

E-commerce crutches are described in figure (2); those represents factors affects the e-commerce environment.



**Figure (2): E-commerce Crutches**

E-commerce technologies are: Electronic Data Interchange (EDI) and Internet. EDI used in B2B and Internet used in B2C (Beck, 2002).

However, EDI refers to the exchange; by using digital media, of structural business information transactions such as purchase orders and invoices between buyers and sellers (Team, 2001). While, Financial EDI is an aspect of electronic payment mechanism involving transfer of funds from the bank of a buyer to the bank of a seller (Hill, 2000).

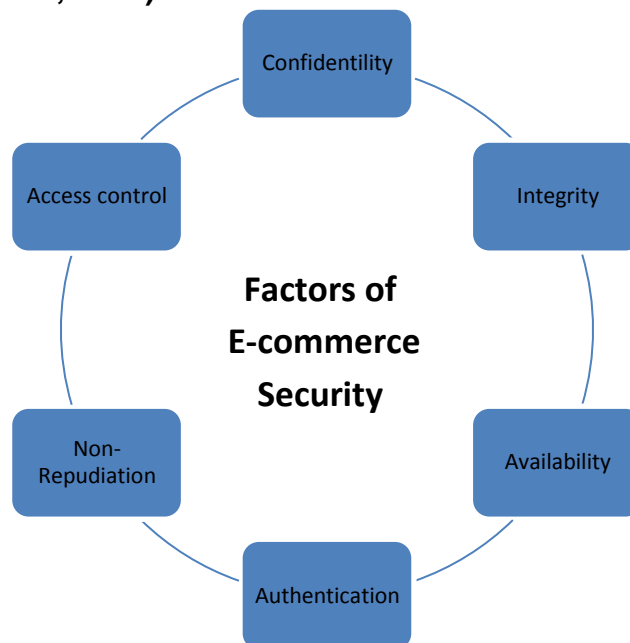
Generally, like other tools EDI have features and limitations. EDI features are: 1.Information exchange and products enquiries, 2.Create bills and enquires about shipping/delivery dates, 3.Using a unified standard for electronic data exchange called UN/EDIFACT, 4.EDI helps in decreasing operations cost, minimize workers, 5.EDI use one of the following techniques for electronic data exchange; e.g. Value Added Network (VAN), using the internet by the tool (EDI/INTERNET), and the second technology used with B2C by using the web site, 6.EDI used to be the most safety technology (Jiang, 2005). On the other hand, EDI limitations are: 1.High cost of used tools, 2.High cost of communications, which have been solved by using the internet (Team, 2001).

However, EDI helped in electronic data transfer; but recently the work started with eXtented Markup language (XML) as another way for electronic data transfer across the internet, so the EDI has been ignored because XML is more flexible than EDI in e-business environment (Team, 2001). XML is a standard for transferring structured data, unlike HTML which is purely presentational [27]. Recently, XML has been improved to fit the requirements of business process, to get ebXML (Team, 2001).

Mainly, there are multiple methods to be used for protecting the electronic environment of businesses. For an example, Virtual Private Network (VPN) used to enable the global organization to conduct its business securely but using the public internet rather than more expensive proprietary systems. However, current approaches to e-commerce security are: SSL, SET, and CA (Hwang, 1999). Secure Socket Layer (SSL) is a commonly used encryption technique for scrambling data as it is passed across the internet from a customer's web browser to a merchant web server. SSL used in B2C. Secure Electronic Transaction (SET) is a standard for public key encryption intended to enable secure e-commerce transactions-developed by master-card and visa (Wang, 2001).

The core idea of multilayer architecture is in separating application service logic from resource and subdividing the function and roles of services (Sarkar, 2009) and (Huy, 2007). Mainly, multilayer architecture improves the reliability, extensibility, and tractability of the system (Wang, 2008). Multilayer applications are; e.g. Model-Driven Development (MDD); Service-Oriented Architecture (SOA) (Kim, 2008); SOA-three layer abstraction; web application with five layer (Wang, 2008).

The network is important for communication and information exchange; especially in e-business environment. But that communication should be secured against an unauthorized person. Mainly there are three main factors that affect securing any system; e.g. confidentiality, Integrity, and availability. But for e-business there are multiple factors or dimensions that affect its security; e.g. confidentiality, Integrity, availability, authentication, non-repudiation, and access control, as in figure (3) (Orsborn, 2008).



**Figure (3): E-commerce Security Factors**

From figure (3), authentication is one of the main factors that affect e-business security. It protects both sides (sender and receiver) from others but it does not protect them from each other. However, to achieve authentication we can use one of the digital signature protocols. Hence, digital signature can be achieved by using a third person (called Arbitrator) this person should be trusted from both sides. This type of digital signature called Arbitrated Digital Signature, where there should be mutual authentication in both side between sender and arbitrator and between receiver and arbitrator. And by using the public-key encryption approaches, the arbitrator (called Key Distribution Center KDC) will be in the middle between initiator (called A) and receiver (called B) to start their communication safely; as in the following scenario: (Stallings, 2006).

- 1- A to KDC :  $ID_A || ID_B$
- 2- KDC to A :  $E_{K_{Rauth}}[ID_B || KU_b]$
- 3- A to B :  $E_{KU_b}[N_b || ID_A]$
- 4- B to KDC :  $ID_B || ID_A || E_{KU_{auth}}[N_a]$
- 5- KDC to B :  $E_{K_{Rauth}}[ID_A || KU_a] || E_{KU_b}[N_a || K_s || ID_B]$
- 6- B to A :  $E_{KU_a}[E_{K_{Rauth}}[N_a || K_s || ID_B || N_b]]$
- 7- A to B :  $E_{K_s}[N_b]$

#### Related Work

In (Nayak, 2001) the paper discussed the author's experiences in developing a web-based infrastructure for creating, operating, and

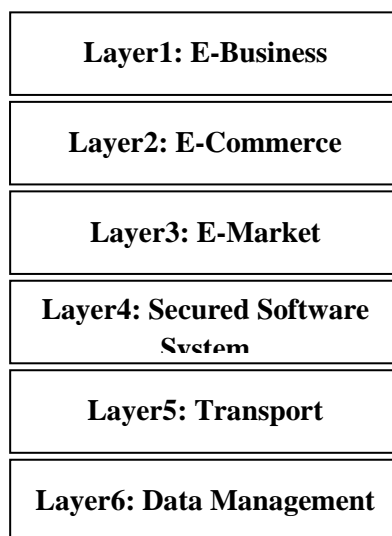
eventually dissolving virtual enterprises. The primary operators of the proposed infrastructure will be market makers offering custom products and services in various industries as well as corporations involved in bringing new products to the market.

In (Hu, 2004) the authors presented a new model for intelligent e-business portal using multiple wisdom web technologies. In (Maciaszek, 2007) a new strategy for modeling and engineering e-business systems; they depended on a six-layer meta-architecture (called PCBMER). In (Shi, 2000) a three-layer virtual e-business framework has been proposed with data mining techniques. In (Rajarman, 2005) proposed another idea of e-commerce as a set of independent six-layers. Each layer, deals with some specific aspect; e.g. physical, logic, network service, messaging, middleman, application.

(Nachtigal, 2007) presented a new model to secure e-business work; Depending on the characteristics of e-business process together with the technological environment; to fit the real security requirements of each process for the whole organization. (Hasseb, 2011) Presented a new approach to secure the communication in e-commerce transactions using simple cryptography techniques. (Haddad, 2007) Defined a new protocol for e-commerce work to minimize the bandwidth and computational complexity for both the customer and merchant.

#### ***Enhanced E-Business Layered Architecture with CTAM***

This paper presents an enhanced e-business infrastructure in the form of multilayer architecture to enable as go through all the details of the electronic business environment; for more flexible and reliable electronic transactions. The propose e-business architecture contains six layers, were each layer constraint's on an important step of the electronic business world. This paper presents "Enhanced E-Business Layered Architecture", as in figure (4):



**Figure (4): Enhanced E-Business Layered Architecture**

However, Layer-1 contains decision making ability depending in the offers and requests, and the services of translating customer's desire to services done by one merchant or more. Layer-2 deals with secured electronic payment with dual signature. Layer-3 deals with analyzing the market status for future forecasting, and Bills creation, with negotiation ability. Layer-4 specialized in security software system to enable secured communications, across the internet. Layer-5 describes the network type to be used as a communication tool; for example ad hoc networks. Layer-6 concerns with storing the data with ability to transport them over the net, so the best structure will be XML files. And retrieve the data in secured way by using Private Information Retrieval (PIR) with the use of data mining algorithms.

As we can see from figure (4), that Layer-4 deals with securing issues. Hence, the communication will be secured by using Customer Trusted Arbitrator Merchant (CTAM) algorithm as in figure (5).

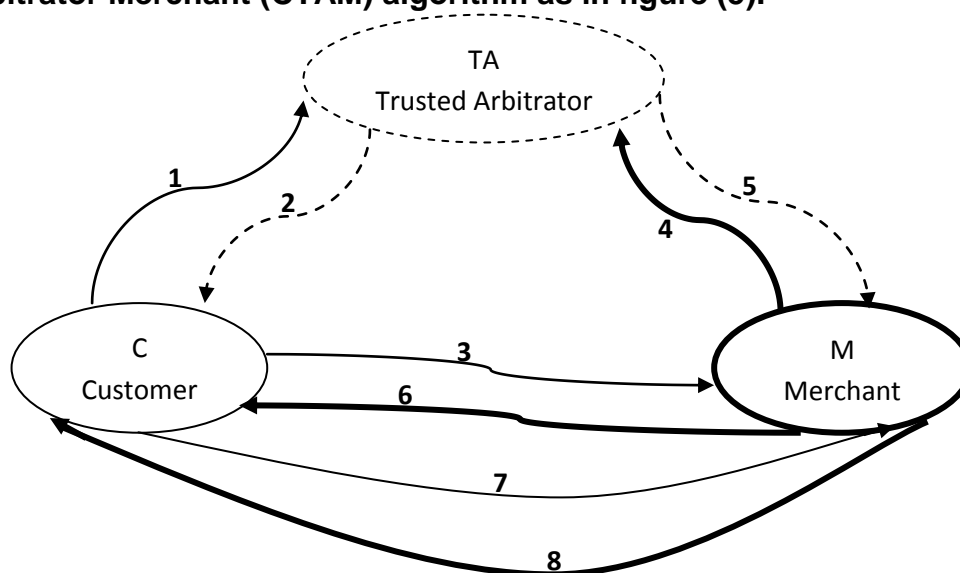


Figure (5): Customer Trusted Arbitrator Merchant (CTAM)

The steps performed by CTAM (shown in figure 4) are:

- 1- The Customer (C) sends request to the third party who called Trusted Arbitrator (TA) to have a Ticket (T) for contacting with the Merchant (M):  $E_{KU_C}[ID_C||Time||N_C]$ .
- 2- TA sends back a reply for C :  $T_c = E_{KR(TA)}[ID_C||Time||N_C||K_c]$
- 3- C sends (Ticket (T) with its public key) to M as a sign to start connection between C and M:  $E_{K_S}(T_c||KU_C)$ .
- 4- M sends request to TA for a Ticket:  $E_{KU_M}[ID_M||Time||N_M]$  .
- 5- TA answers M with a reply contains the Ticket to be used by M:  $T_M=E_{KR(TA)}[ID_M||Time||N_M||K_s]$ .
- 6- M uses the Ticket to answer C:  $E_{K_S}[T_M||KU_M]$ .
- 7- C starts to communicate with M by sending its request encrypted with its private key:  $E_{KU_M}[N_1||E_{KR_C}(Req_c||Time)]$ .
- 8- M sends back its answer to C encrypted with the private key of M:  $E_{KU_C}[N_2||E_{KR_M}(Rep_M||Time)]$ .

## Implementation and Results

This paper presented CTAM algorithm to secure the transaction in the proposed layered architecture for E-Business operations. The algorithm is implemented by using Windows Presentation Foundation (WPF) of .Net environment; e.g. C# language, as in figures (6 and 7). Moreover, the information was stored using eXtensible Markup Language (XML) as in the figures (8, 9, and 10). XML is both human readable and machine readable also it has the same a tree structure that means it has a constant search time for any file size.

Figure 6, shows the six-layers for the proposed architecture, in this paper we have presented the work for the fourth layer (Secured Software Layer) as in figure (7).

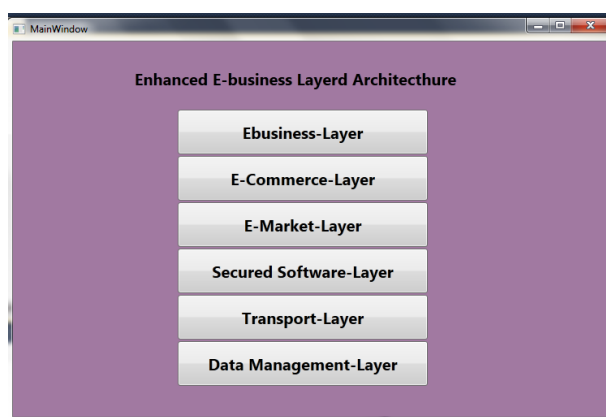


Figure (6): Main Menu for the Proposed Architecture

Figure (7), is an implementation for the CTAM algorithm which starts with pressing the C-command in the main. This command represents starting the transaction between the three parts (Customer C- Trusted Arbitrator TA-Merchant M). In the same menu we can see three text boxes to view the details for each side; that information will be stored in its corresponding XML file.

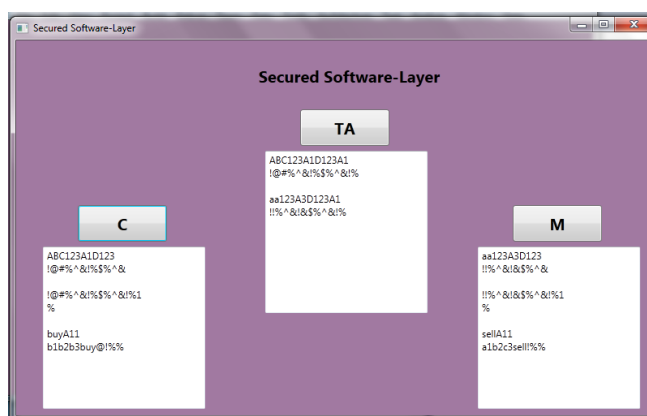
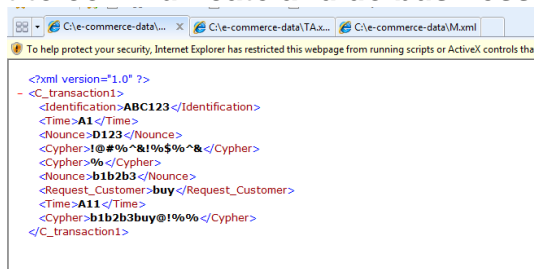


Figure (7): CTAM menu

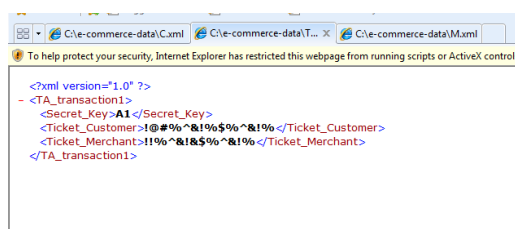


Figures (8,9 and 10) presents the data of the CTAM algorithm between the three parts; sender C, receiver M, and third trusted parity TA. Where C wants to communicate with M but the second one does not trust C but M trusts TA and also C. Hence, C communicates with TA to have a ticket with limited life time to start a trusted session with M. In the same time M will do the same as soon as the Ticket reached to the M side. Finally both sides will start to communicate and do business.



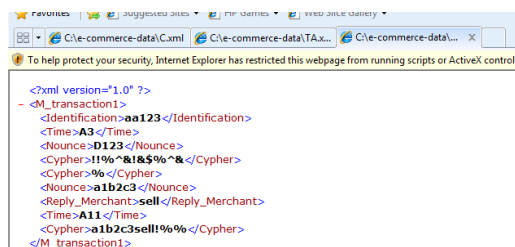
```
<?xml version="1.0" ?>
<C_transaction1>
  <Identification>ABC123</Identification>
  <Time>A1</Time>
  <Nounce>D123</Nounce>
  <Cypher>1@#%&1%$%^&</Cypher>
  <Cypher>%</Cypher>
  <Nounce>b1b2b3</Nounce>
  <Request_Customer>buy</Request_Customer>
  <Time>A11</Time>
  <Cypher>b1b2b3buy@1%</Cypher>
</C_transaction1>
```

Figure (8): Customer (C) File



```
<?xml version="1.0" ?>
<TA_transaction1>
  <Secret_Key>A1</Secret_Key>
  <Ticket_Customer>1@#%&1%$%^&1%</Ticket_Customer>
  <Ticket_Merchant>11%&1&1%$%^&1%</Ticket_Merchant>
</TA_transaction1>
```

Figure (9): Trusted Arbitrator (TA) File



```
<?xml version="1.0" ?>
<M_transaction1>
  <Identification>aa123</Identification>
  <Time>A3</Time>
  <Nounce>D123</Nounce>
  <Cypher>11%&1&1%$%^&1%</Cypher>
  <Cypher>%</Cypher>
  <Nounce>a1b2c3</Nounce>
  <Reply_Merchant>sell</Reply_Merchant>
  <Time>A11</Time>
  <Cypher>a1b2c3sell@1%</Cypher>
</M_transaction1>
```

Figure (10): Merchant (M) File

## Conclusion

The internet which is the main medium used for managing e-business transactions, is not designed to enhance its performance, for example securing its transactions. This paper presents an enhanced E-business architecture that contains CTAM algorithm to secure transaction process for its users. The CTAM algorithm used to increase the level of security by using some cryptography techniques.

## References

1. Beck V.R. Innovation Systems and Impact of E-commerce and EDI on German SME, Institute of Information Systems, Johann Wolfgang Goethe University, 2002.
2. Chaffey Dave E-Business and E-Commerce Management *second edition*, Prentice Hall, 2004.



3. Chong W.K., Tadjouddine E.M., Shafaghi M., and Tan B.L. Automated Mechanism Design for B2B e-Commerce Models, International Journal of Trade, Economics and Finance, Vol.2, No.1, February, 2011.
4. Haddad E. and King B. A Simple Secure M-Commerce Protocol SSMCP, International Journal of Computer science and Network Security, Vol. 7, No. 3, 2007
5. Haseeb K., Arshad M., Ali S., Yasin S. Secure E-Commerce Protocol, Department of Computer Science, Islamia College University, International Journal of Computer Science and Security, Volume 5, Issue 1, 2011.
6. Havyatt David Competition Policy for the Digital Economy, DIGECON, 2011.
7. Hill N.C. EFT and EDI, Brigham Young University, 2000.
8. Hu J., Zhong N. Organizing Dynamic Multi-Level Workflows on Multi-Layer Grids for Developing E-Business Portals, IEEE, 2004.
9. Huy Pham, Qusay Mahmoud, Alexander Ferworn, and Alireza Sadeghian Applying Model-Driven Development to Pervasive System Engineering, First International Workshop on Software Engineering for Pervasive Computing, IEEE, 2007.
10. Hwang S.O., Choi Y.B., Lee J.S. Yoon K.S., and Kim M.J. Recent Industrial Development of VPN (Virtual Private Network), China 1999.
11. Jiang L., Xu B., and Ma F. On the new B2B E-business Enabling Platform-cnXML in China ACM, 2005.
12. Kim Jong-Hwan, Jeong In-Bae, Park In-Won, and Lee Kang-Hee Multi-Layer Architecture of Ubiquitous Robot System for Integrated Services, Springer, 2008.
13. Lau Raymon Y.K. Adaptive Negotiation Agents for E-business, Department of Information Systems, City University of Hong Kong, ACM, China, ICEC'05, 2005.
14. Maciaszek L.A. Modeling and Engineering Adaptive Complex Systems, 26<sup>th</sup> International Conference on Conceptual Modeling – ER 2007.
15. Montgomery E., E-commerce Features, graphxevolution, 2009.
16. Nachtigal S. eBPSM- A New Security Paradigm for E-Business Organizations, Information Security Group, Royal Holloway, University of London, ACM, 2007.
17. Nayak N., Bhaskaran K., Das R. Virtual Enterprises-Building Blocks for Dynamic E-Business, IEEE, 2001.
18. Orsborn Kjell E-Commerce and Security, Uppsala University, Sweden, Spring 2008.
19. Rajarman V. Building blocks of E-Commerce, Supercomputer Education & Research Center Indian Institute of Science, 2005.
20. Santti Roosa-Maria Technology Acceptance factors in E-commerce Environment – Case DHL Express, Master's Thesis, Department of Information and Service Economy, Aalto University, School of Economics, 2011.
21. Sarkar Santonu, Maskeri Girish, Ramachandran Shubha Discovery of architectural layers and measurement of layering violations in source code, ESELVIER, 2009.
22. Shi A., Long A., and Newcomb D. Enhancing E-Business Through Web Data Mining, South Bank University, 2000.

23. Stallings William Cryptography and Network Security principles and practices *fourth edition*, PEARSON, Prentice Hall, 2006.
24. Team T.A. Technical Architecture Specification, OASIS, 2001.
25. Wang Yiqiao, McIlraith Sheila A., Yu Yijun, and Mylopoulos John Monitoring and diagnosing software requirements, Springer, 2008.
26. Wang Yun and Li Yang Secure Electronic Transaction (SET protocol), china, 2001.

.....  
.....  
.....