I.J. Information Technology and Computer Science, **2016, 01, 67-73**
Published Online January 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.01.08

Double Securing from Hackers in B2B E-commerce

Samara Mubeen
J.N.N. College of Engineering/Information Science and Engineering, Shimoga, 577201, India
E-mail: samaramubeen7860@gmail.com

Srinath N.K. and Subramanya K.N.
R.V. College of Engineering/Computer Science and Engineering, Bangalore, 560059, India
E-mail: srinathnk@rvce.edu.in, sansa96@gmail.com

Abstract—Business to Business e-commerce is adopted by more and more companies all over the world. Many companies will be involved in doing business over internet among them some will act as manufacturer and other as suppliers of the sub products. Here we are going consider two types of hackers**,** the hackers who are outside the organization and the hackers present within the organization. The problem is how to identifying authentic supplier and to see that after authentication the data integrity, here we consider it as the number of sub product to be manufactured that should reach the authentic supplier in the presence of hacker within the organization. There is need for designing trusted security framework. In this paper we are designing a security framework which runs double securing algorithm by using keyless cryptography algorithm for finding the authentic supplier and to see that the order of sub product to be manufactured reaches correct supplier for this caser cryptography algorithm is used. The authentication solves the problem of outside hackers and uses of caser cryptography solve the problem of hacker within the organization. The double securing algorithm is implemented on MATLAB, CPU time is calculated to known the time taken to run the security mechanism.

Index Terms—Business to Business e-commerce, keyless cryptography, caser cryptography, security framework, authentication, data integrity.

I. INTRODUCTION

The traditional way of buying and selling of product are going off these days due to the busy schedule and busy life style. This has given way to easy and upcoming type of commerce called e-commerce. E-commerce refers to paperless exchange of business using internet technologies. Business to Business is one of the branches of e-commerce in which business is carried out between business companies. The transaction can take place between manufacturer and wholesaler, manufacturer and suppliers or wholesaler and retailers. Here we are considering the transaction between manufacturer and suppliers in which a single manufacturer in ordering for the sub product which are to be manufactured by the suppliers. For security in business to business cryptography is used. Cryptography can be divided into two major forms. They are symmetric key cryptography, asymmetric key cryptography.

In symmetric key cryptography same key is used for encrypting and decrypting the message. Some of the algorithm which use symmetric algorithm are two fish, advanced encryption standard, blowfish, Caesar ciphers etc.

In Asymmetric key cryptography different keys are used for encryption and decryption of the message. By using public key message is encrypted and decryption is done using the private at the destination. Public key is easily available to all without any u. Data encryption standard, RSA, elliptic curve algorithms are some of the algorithm which make use of asymmetric key cryptography. Digital signatures are also the part of asymmetric key cryptography which has three procedures. In the key generation procedure private key and public key are generated, a signing procedure in which a message and private key produce a signature and last procedure is signature verifying procedure in which given the message, public key and signature, depending on the authentication the message will be either accepted or rejected.

The hackers are very smart enough to hack the key whether the manufacturer and suppliers use the symmetric cryptography or asymmetric cryptography. There is a need to design a security framework for obtaining authentication, data integrity and securing the transaction between the suppliers and manufacturer such that it becomes impossible for the hacker to get the key and finally the message. The flow of paper consist literature review in section II, business to business e-commerce business model and security algorithm in section III, result and analysis in section IV and finally conclusion in section V.

II. LITERATURE REVIEW

Cryptography based e-commerce Security A review, Shazia Yasin et.al, security is a very important issues of E-commerce, in this paper security based on pretty good privacy (PGP). PGP can be used to provide authentication and confidentiality. But it is not full proof solution because integrity, non-repudiation and replay threats are also important e-commerce security dimensions. Secure E-commerce protocol provides protection to a single transaction at a time it cannot handle multiple E-commerce transactions at a time [7].

E-commerce security using new public key algorithm based on block cipher, Prakash Kuppesswamy et.al. New public key algorithm is proposed having the customer, trusted third party and lastly the merchant [8]. This algorithm is compared with other algorithm which shows the time taken is less on the number of characters against different algorithm.

The study of information security in e-commerce application, Mohammed Ali Hussain, E-commerce two types of encryption methods offer symmetric and asymmetric. The security threat of e-commerce includes viruses, worms, Trojan horse, denial of service, password [3]. The technologies for protecting e-commerce transaction include encryption of data, SSL, digital signature certificates smart card, e-cash.

E-commerce system: A review on security challenges and Indian perspective, Journal of information knowledge and Research, Hardik Nariya, Chirag Gohel [2], the paper explains types of attacks in e-commerce and different security mechanism to tackle online fraud attacks in e-commerce.In one more paper E-commerce security, Nada M.A, Al-Slamy [4], Pretty good privacy is used for e-commerce. It has five services authentication and confidentiality.

III. Business to Business E-Commerce Buisness Model

The literature review shows that only one form of cryptography method is used for securing the communication or the transaction in e-commerce. In which the hacker can hack the key and get important message being communicated between the two parties. Business to business e-commerce is the vast concept as stated earlier we consider transaction taking place between suppliers and manufacturer. In this paper we are dividing the hackers into two types, hacker who are present outside the organization and the hacker present within the organization. Double security algorithm is designed here by which we avoid the hackers present both inside the organization and outside the organization. The double security algorithm makes use of two type of cryptography concept to achieve data integrity and authentication. One algorithm is keyless cryptography and other is caser cipher algorithm.

The suppliers are assigned supplier-ID by the manufacturer depending on their reputation or it can assign randomly for example S1 for supplier1, S2 supplier 2 etc. Here the supplier-ID is assigned randomly. The messages being communicated are given below

1. Request message is the broadcast message by the manufacturer.
2. Acknowledgement message is the messages send by the suppliers back to the manufacturer.
3. Send order message is the message send by the manufacturer giving the information about the number of sub product to be manufactured by the suppliers.
4. Receive order message is the message received by the manufacturer getting the information about the sub product manufactured.

A. Business Model without security with in single organization

The business model considered in this paper has a manufacturer and N number of suppliers. The manufacturer broacast the request message to all the suppliers. If the supplier does not want to manufacture the sub product supplier will not send the acknowlegement message. Hackers may hack the information from the manufacturer and may manufacture sub product which manfacturer will think it is done by the supplier whom he has selected. The same is shown in the figure 1.

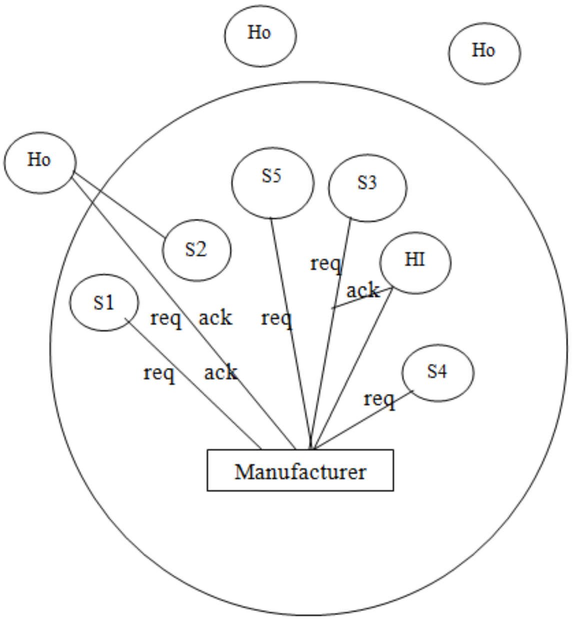

Fig.1. Buisness Model Without Security

The above business model is without security mechanism shows the manufacturer, S1,S2,S3,S4,S5 as suppliers, HI hacker within the list of suppliers but is not selected for supplying sub products and Ho is the hacker who not in the list of the manufacturer and Ho is the hacker who not in the list of the manufacturer. There are two messages being communicated between the manufacturer and the supplier. They are req which is request message, ack the acknowledgement message , so is the send order message contains the number of subproduct to be manufactured by the suppliers, and ro is the receive order message the manufacture gets the sub product from the suppliers. The manufacturer broadcast the request for manufacturing of the sub product to the all suppliers.

The supplier S2 will not get the information about the selection of it by the manufacturer, its message is hacked by the outside hacker Ho, he communicate with the manufacturer as if it is supplier S2 here the authentication is required.The S3 will get the request message and send ack message to the manufacturer, on receiving this manufacturer will send the send order message which contains the sub product to be manufactured, this message is used by the hacker HI who will communicate on behalf of supplier S3. S3 will not get the message of send order. Here is the need for data integrity.

The supplier S5 and S4 are not going to manufacture sub product so they will not send the acknowledgement message back.

B. Business Model with double security within single organization

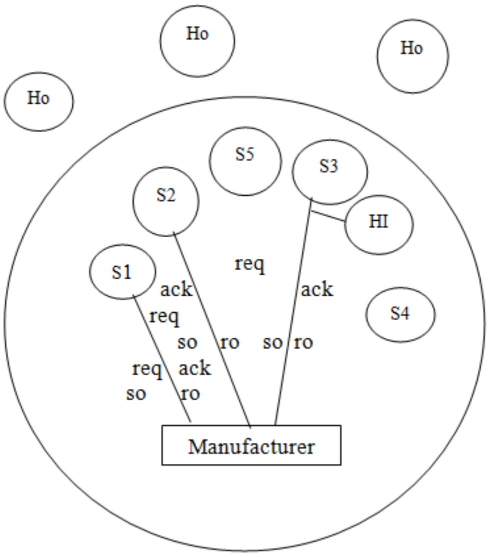

Fig.2. Buisness Model with Security

In this business model the manufacturer carefully selects suppliers based on the quality of sub product, time the sub products are delivered etc and other aspects. There are four transactions of messages between the suppliers and manufacturer. The messages are req message is the request message, ack message is the acknowledgement message, so is the send order message and ro is the receive order message. The manufacturer instead of broadcasting the messages send the request message to the specific supplier in the above diagram it is S1, S2, S3 from this authentication of the supplier is achieved. The inside hacker will know the communication between the S3 and the manufacturer but is not able get the information about the number of sub product to manufacture as this information is again send by the manufacturer to the authentic supplier in the form of send order and finally the manufacturer will receive the order of sub product. Like this data integrity is obtained. During authentication process keyless cryptography is used then after confirmation that the request has reached the authentic supplier then for send order one more cryptography algorithm is used, here it is caser cryptography.

C. Business Model with out security between two organizations

In this case study we are going to consider the communication or transaction taking place between two different organization manufacturing same type of final product to same company. We assume that due to the shortage of suppliers within the organization the manufacturer request the suppliers of other organization.

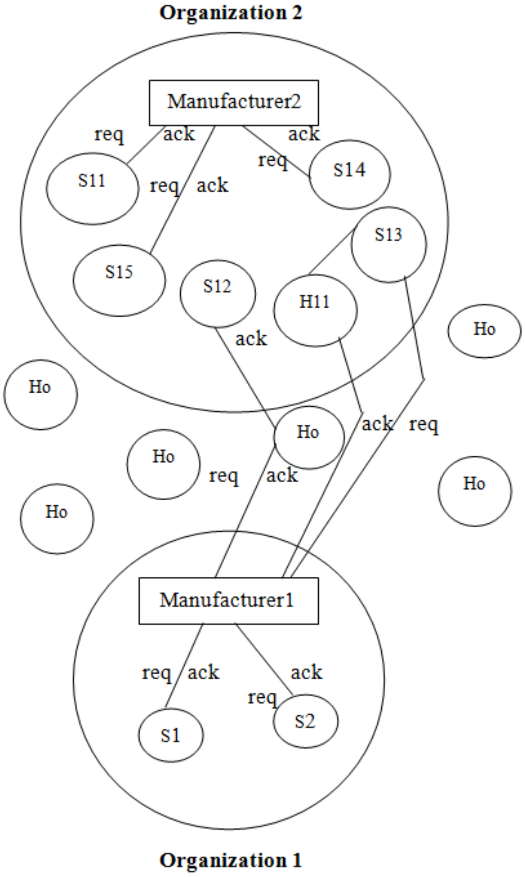

Fig.3. Buisness Model with Out Security Between Organizations

The business model shown above has two organizations namely organization1 and organization2. We assume that the organization1 is new organization and has limited supplier with it, even the diagram shows that manufacturer1 has only two suppliers S1 and S2. Organization1 has shortage of suppliers for manufacturing the sub products; it takes the help of the other organization here its organization2. The manufacturer1 broadcast the request message to the suppliers present in the both organizations. The suppliers of organization2 who are not selected can participate in manufacturing the sub products. During this the hackers will hack the request message transmitted by the manufacturer1 which should reach supplier S12 of organization2. The manufacturer1 unaware of the fact will accept the ack message and send the order for manufacturing of sub product to the hacker Ho who is in track of the communication between the two organizations instead of the actual supplier S12. There is one more hacker H1 present inside the organization2, the broadcast message send by the manufacturer1 is received by the supplier S13 of the organization2. The hacker H1 hacks the broadcast message send the ack message in behalf to supplier S13. Again the manufacture1 believes that the ack message is received by the correct supplier and involve in doing business. in this way the hacker present outside and inside the organizations are involved in manufacturing sub products.

D. Business Model with double security between two organizations

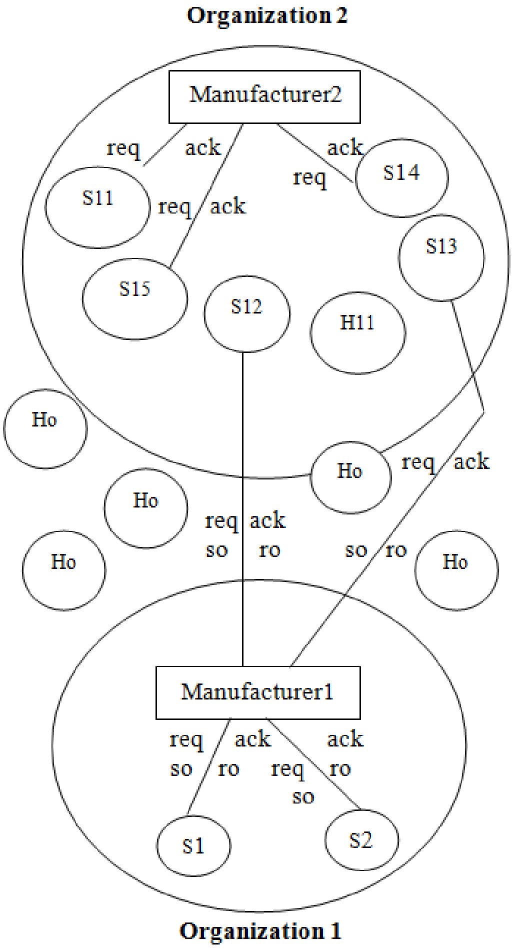

Fig.4. Buisness Model with Security Between Organizations

The organization2 is having five supplier S11, S12, S13, S14 and s15 respective and the organization1 is having the supplier S1 and S2 only, it still require more suppliers.The manufacture1 of the organization1 will identy the suppliers who are free and not involved in manufacturing of the sub product belonging to the organization2, in diagram the supplies S12 and S13 are free. Manufacturer1 will take put their supplier ID and the supplier ID of the supplier in organization1 who are supplier S1 and S2 in a file and send it as a request message. This time request message reaches the specified suppliers and not all.Like this the hacker Ho is prevented from hacking the request message. The hacker H1 present inside the organzation2 will know that there is transaction taking place between the supplier S13 and manufacturer1 of the organization1 but his effort goes in vain as the manufacturer use on more cryptography alogrithm to encrypt the message which contain number of product to manufacture and is send in the form of send order (so) message. The respective suppliers after getting the message of send order will send back the message about the recipent of the message back to the manufacturer1 of the organization1 in form of recive order (ro) message. Like this using double security mechanism the both hackers are avoided completely. We apply the double security only to organization1 and we are not worried about what security mechanism adopted by organization2 and its manufacture2 and their suppliers.

The double security algorithm for business to business is given below

```
1. Start
2. Manufacturer selects the suppliers wisely and send the
   request message using keyless cryptography.
3. After getting acknowledgement message the number of
   sub product to manufacture is send to suppliers, for data
   integrity caser algorithm is used.
4. Total time required to run the security algorithm is got.
5. Best suppliers are selected depending on the sub product
   being manufactured or the time taken to run the security
   mechanism.
6. End.
```

Algorithm 1. Security Algorithm of Business to Business

The algorithm shows that the suppliers who are selected by the manufacturer carefully are enclosed in a file along with their ID, by using the keyless algorithm they are send to the suppliers on receiving this supplier's send acknowledgement back to the manufacturer. The manufacturer then uses caser algorithm to encrypt the information as the number of sub product to be manufactured like this data integrity is achieved. The hackers outside the organization and within organization are completely eliminated.

The same algorithm is applied for transaction taking place between two organizations manufacturing same type of product. The new organization having shortage of supplier's can take the help of the supplier present in different organization, here also the hackers present within and outside the organization can be prevented.

IV. Result and Analysis Buisness Model

The algorithm given above is run for simplified model having a manufacturer and two suppliers only and case study B is used. The two suppliers are selected randomly from among the available ten suppliers. Since the suppliers are selected randomly either two suppliers or one supplier are selected every iterations. We are going to analysis the result in three ways, first is selection of best suppliers in number of order terms of sub product manufacturing is maximum, second in terms of minimum time taken to run the secure algorithm and third considering both number of order item and minimum time required for running the algorithm.

A. Selection of suppliers in term of number of sub product order item.

The table 1 shows three columns one is number of iteration, second is the supplier ID which contain the identification number of the supplier who is selected for manufacturing sub product and last column shows that order item which gives the information about the number of sub product to be manufactured by the supplier. The ten iterations, suppliers present are ten from them only two suppliers are selected randomly and authenticated supplier is given the order to manufacture the sub product by the manufacturer.

Table 1. Supplier Involved in Processing the Order

Iteration	Supplier ID	Order item
1	S1	453
2	S6	200
3	S8	101
4	S3	115
	S2	101
5	S5	222
6	S9	666
	S4	650
7	S6	666
	S4	650
8	S2	550
	S4	999
9	S5	141
10	S2	222

Consider the first iteration in which only one supplier having the supplier ID S1 is selected and number of sub product it is going to manufacture is 453. Now consider the iteration 4 in which two suppliers are selected with supplier ID S3 and S2 and they are going to manufacture 115 and 101 sub product respectively.

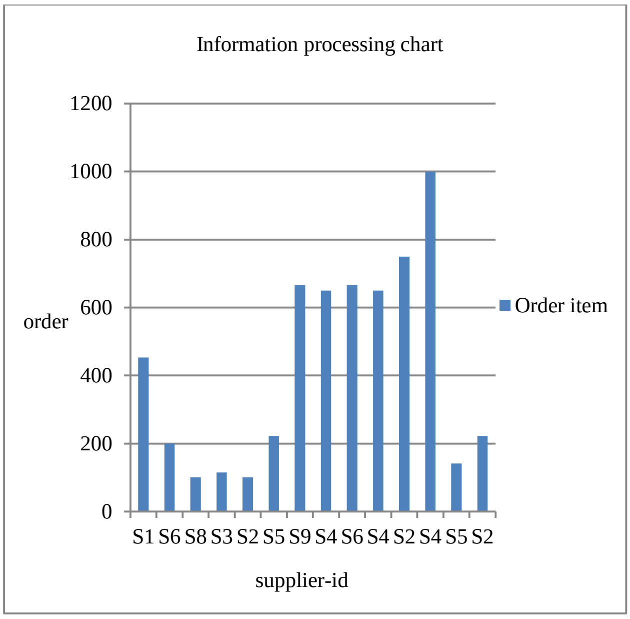

Chart 1. Selection of Respective Supplier for Processing Information

The chart 1 shows the selection of the suppliers after running the double security algorithm. Here by using the information from the chart1 we can select supplier depending on the number of sub product being manufactured. The manufacturer can also decide whether it wants one supplier or two suppliers for manufacturing sub product. From the chart1 in iteration 8 in which two suppliers are selected S2 and S4 who are going to manufacture more sub product compared to other suppliers in which two suppliers are involved. The manufacturer wants to select one supplier then it will S1 in first iteration as it manufactures more sub products. The manufacturer after running the secure algorithm has the chance of selecting the best suppliers and also number of suppliers either one or two. In the above analysis the manufacturer if he wants two suppliers will select S2 and S4 suppliers and if only one supplier is enough then he selects supplier S1.

The same process can be carried out in the selection of the suppliers by the manufacturer in the above cases that has been discussed that is in business model with double security within single organization and business model with double security between two organizations**.**

Th**e** manufacturer will have faithfully and trustworthy suppliers as the double security algorithm are run. The manufacturer will get the sub product manufactured at the correct time.

B. Selection of suppliers in term of time taken to run the secure algorithm

The table 2 shows the two columns having number of supplier involved during each iteration in the same business model having one manufacturer and N supplier, where the value of N is ten here. Out of the ten suppliers present two suppliers are selected as the model is one manufacture and two suppliers. The second column shows time taken by the CPU for running the double secure algorithm when respective suppliers are selected.

Table 2. Total Time Taken for Security Session

Number of supplier involved	Time taken by the CPU for processing in seconds
1	0.09375
1	0.0156
1	0.031250
2	0.125
1	0.03125
2	0.0625
2	0.09375
2	0.1875
1	0.01965
1	0.0312

The manufacturer who not interested on the number order items can select the supplier's depending upon the time taken for executing the algorithm.

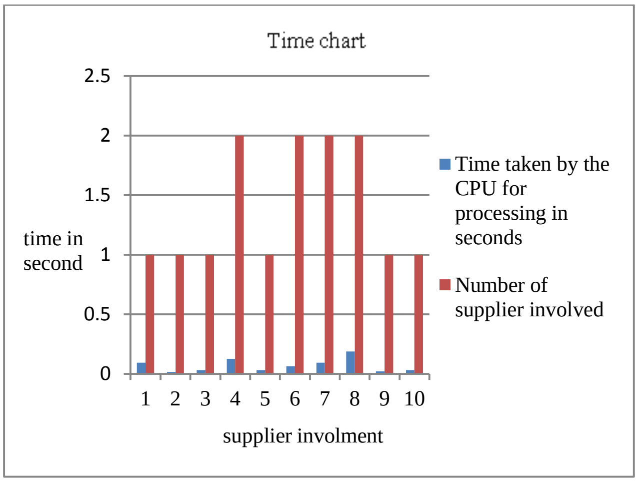

Chart 2. Selction of Respective Suppliers for Processing Information

From the table1, table2 and the chart 2 if the manufacturer wants to select the supplier in terms of time taken to run the security algorithm then for one supplier it is supplier with supplier ID S6 in the iteration 2 and time taken is 0.0156 seconds and for two suppliers it the six iteration the supplier's are S9 and S4 and time taken is 0.0625 seconds.

C. Selection of suppliers in term order item and time taken to run the secure algorithm

Manufacturer who wants to make best selection of supplier after running double security algorithm will select the suppliers based on both the factors, minimum time taken by the CPU and order item for running the secure algorithm. By looking at table1, table 2, chart 1, chart2 if one supplier is to be selected it would be supplier with supplier S6 as the time take is minimum its 0.0156 seconds and order item is maximum compared to other suppliers its 200. When two suppliers are to be selected it will be suppliers having supplier ID S9 and S4 where the time taken is 0.0625 and order item is 666 and 650 respectively. Here we first look at minimum time in each iteration then search for the supplier ID having order item.

V. Conclusion

The business to business e-commerce is upcoming trend where the business transaction takes place between the business partners, which has given a way for hackers. The business model considered here are two one is a manufacturer and one or more suppliers and other is between two organizations manufacturing same product and is shortage of supplier. Keyless cryptography is used for avoiding hacker outside; authentication of the selected supplier's is achieved. To obtain the data integrity caser algorithm is used. By running the double secure algorithm the manufacturer gets a chance to select the supplier's in terms of number of sub product manufactured by the supplier's or in the terms of time taken to run the double security algorithm. Result and analysis is carried for just two supplier's and a manufacturer in future work it can carried between any number of manufacturer's and any number of supplier's. In future work any other cryptography concept can be applied for carrying on the transaction in business to business e-commerce and helping the manufacturer to make a decision for selecting the suppliers.

References

[1] Casassa Mont M. and Brown, "Pastel Project: Trust Management, monitoring and policy driven authorization framework for E-services in internet based B2B environment" HPL 2001.

[2] Hardik Nariya and Chirag Gobel, "E-commerce system: a review on security challenges and Indian perspectives", Journal of Information Knowledge and Research, 2013, vol 2, issues 2, pp: 451-457.

[3] Mohammad Ali Hussain," A study of information security in E-commerce application" International Journal of Computer Engineering Science, 2013, vol 3, issues 3, pp: 1-9.

[4] Nada M.A. and Al-Sammy," E-commerce Security", International Journal of Computer Science and Network Security, 2008,vol 8, issue 5, pp 340-344.

[5] Raducanu Razvan and Omusaru Edvard," On security of E-commerce", Recent Advance in mathematics and computer in Business, Economics, Biology and Chemistry, ISSN 1790-2769.

[6] Seven Wohlgemuth et.al. "Security and Privacy in business networking Electronic Market", 2014, pp: 81-88.

[7] Shazia Yasin et.al, "Cryptography based security: a review of security challenge and perspective", Journal of Information Knowledge and Research, vol 2, issue 2, pp: 451-457.

[8] Thedosis Toiakis and George sthephanides, "The concept of security and trust in electronic payment", Jornal of Computer Secuirty, 2005, pp: 10-15.

[9] Zoran V. and Milorad, "Simulation Analysis of protected B2B E-commerce process", Comsis vol 3, issue 1, pp: 78-91.

[10] Prakash Kuppaswamy, Saeed Q.Y. Al-Khalvali," Hybrid Encryption/ Decryption Technique using new public key and symmetric key Algorithm", MIS Review, vol 19, issue 2, 2014, pp: 1-13.

[11] Farah Hanna Zawaideh, "E-commerce Secure Transfer based on embedded DSP", International Journal of Latest Research in Science and Technology", vol 2, issue 2, pp: 124-128, April 2013.

[12] Akhilesh Dwivedi et.al, "A Cryptography algorithm analysis for security threats of semantic E-commerce web for electronic payment transaction system", Advances in computing and information technology, pp: 367-378, 2013.

[13] Pita Jarupunphol and Wipawan Buathong, "Secure Electronic Transactions (SET): A case of Secure System Project failures", International Journal of Engineering and Technology, vol 5, issue 2, April 2013.

[14] Raghav Gautam and Sukhwinder Singh, "Network Security issues in E-commerce", International Journal of Advanced research in Computer Sceince and Software Engineering", volume 4, issue, 3, March 2014, pp: 130-132.

[15] Pradnya B. Rane et.al, "Authentication and Authorization: Tool for E-commerce security", Engineering Science and Technology: An International Journal, volume 2, issue 1, 2012.

[16] Elminaam, D.S.A., Kader, H.M.A. and Hadhoud, M.M., "Evaluating the performance of symmetric encryption

algorithms", International Journal of Network Security, Vol. 10, No. 3, pp. 213-219, 2010.

[17] Kuppuswamy, P. and Al-Khalidi, S.Q.Y., "Implementation of Security through simple symmetric key algorithm based on modulo 37", International Journal of Computers & Technology, Vol. 3, No. 2, pp. 335-338, 2012.

[18] Ramaraj, E., Karthikeyan, S. and Hemalatha, M., "A design of security protocol using hybrid encryption technique", International Journal of the Computer, the Internet and Management, Vol. 17, No. 1, pp. 78-86, 2009.

[19] Trust Services: A Trust Infrastructure for E-Commerce, Adrian Baldwin et al, Trusted E-Services Laboratory, HP Laboratories Bristol, HPL-2001-198, August 2001.

[20] Bakos, J.Y., Brynjolfsson, E., "From vendors to partners: Information technology and incomplete contracts in buyer–supplier relationships", Journal of Organizational Computing, volume 3, pp: 301–328, 1993.

[21] Khalid Haseeb et.al. "Secure E-commerce Protocol", International Journal of Computer Science and Security, Vol. 5, issue. 1, pp.742-751, April 2011.

[22] S. R. S. Kesh and S. Nerur, "A Framework for Analyzing E-Commerce Security," Information Management and Computer Security, volume 10, issue 4, pp. 149-158.

[23] J. J. Amador, and R. W. Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", International Journal of Imaging and Technology, Vol. 15, issue. 3, pp. 178-188, 2005.

[24] C.-S. Laih, and K. Y. Chen, "Generating visible RSA public keys for PKI", International Journal of Information Security, Volume 2, issue 2, Springer-Verlag, Berlin, pp. 103-109, 2004.

[25] Izumi M et.al., "A new approach for implementing the MPL method toward higher SPA resistance", International Conference on Availability, Reliability and Security, pp. 181—186, March 2009.

[26] Hu J, Xi Z, Jennings A, Lee HYJ, Wahyudi D," DSP application in e-commerce security", Processing of IEEE International Conference on Acoustics, Speech, and Signal, pp. 1005—1008, 2001.

[27] Prakash Kuppuswami, peer mohmmad appa, dr.saeed Q. Y. Al khalidi, "A new efficient digital signature scheme algorithm based on Block cipher" IOSR journal of computer engineering ISSN: 2278-0661, vol.7, pp. 47-52, nov-dec2012.

[28] Neetesh sexena and Narendra S. Chaudhary "secure Encryption with the digital signature Approach for short message services", IEEE, 2012.

[29] Kaur Ranveer and Amandeep Kaur, "Digital Signature", IEEE2012 International conference on Computing Science, 2012.

[30] Junling Zhang "A study on Application of digital Signature Technology", international Conference on Networking and Digital society, IEEE 2010.

[31] J. Daemen and V. Rijmen, "Rijndael: the advanced encryption standard," Dr. Dobb's Journal, vol. 26, no. 03, pp. 137-139, 2001.

[32] Karima Mahdi, Raida Elmansouri, Allaoua Chaoui, "On transforming business patterns to labeled Petri nets using graph grammars", International Journal of Information Technology and Computer Science, vol. 5, no. 02, pp. 15-27, 2013.

[33] Mutlaq B.Alotaibi, "E-commerce Adoption in Saudi Arabia: an assessment of International, Regional and Domestic web presence", International Journal of Information Technology and Computer Science, vol. 5, no. 02, pp. 42-56,2013.

[34] Rath Jairak, Prasong Praneetpolgrang, Nivet Chirawichitchai, A Roadmap for Establishing trust management strategy in E-commerce services using quality based assessment", International Journal of Information Engineering and Electronic Business, Vol.6, No.5, PP.1-9, 2014, DOI:10.5815/ijieeb.2014.05.01.

[35] Prema Kumar Balaramma, Kalpana Kosalram, "E-commerce Evaluation and E-Business Trends", International Journal of Information Engineering and Electronic Business, Vol.4, No.5, pp. 9-16, October 2012.

Authors' Profiles

Mrs. Samara Mubeen Assistant Professor in Department of Information Science of Engineering of JNNCE College. I am research scholar, pursuing research in B2B technology, strategy involved in the B2B market, building framework model and performance analysis in B2B market using analytical tool. Published papers in reputed international Journals.

Dr.N.K.Srinath, Dean of Computer Science and Engineering of R.V.College of Engineering. Expert in Database management, System Software, Microprocessor, System Engineering and Operation research. Written books on Microprocessor. Published excellent papers in reputed International Journals.

Dr. K.N.Subramanya, Principal of R.V. College of Engineering. Expert in Supply Chain Management, E-commerce, B2B E-commerce, E-Commerce, Traditional and cloud supply chain, B2B market Design. Published more than ten papers in most reputed international Journals.

How to cite this paper: Samara Mubeen, Srinath N.K., Subramanya K.N.,"Double Securing from Hackers in B2B E-commerce", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.1, pp.67-73, 2016. DOI: 10.5815/ijitcs.2016.01.08