A Survey of various Online Transaction Applications & Security

Md Nadeem Ahmed
Research Scholar
IFTM University, India
mdnadeemahmed.86@gmail.com

Prof Dr Mohd Hussain
mohd.husain90@gmail.com
MGMIT, Lucknow, India

Abstract— Due to rapid development in the field of Internet application, protection of these data is an important issue during the transmission from one end to another end i.e. between sender and receiver especially in web based applications like Online Transaction and E-commerce. Since various techniques are implemented to provide security and authentication to online transactions. Here in this paper various techniques that are implemented for the security and authentication of E-Commerce applications are discussed and analyzed their various advantages and issues in the technique. The various issues or limitations in the existing technique can be removed, hence a complete survey and their advantages and issues is analyzed here so that on the basis of their various advantages and limitations a new and efficient technique is implemented in future. For the betterment of the Security of Online Applications Two Factor based authentication techniques are implemented so that security from various attacks can be possible. Smartphone now a days are very common to everyone and it is widely accepted. It is used for e banking application almost all confidential data is stored in Smartphone which leads to sophisticated attack like eurograbber which happens through mobile botnet installation.

Index Terms— data mining, factor authentication, security model, online transaction, web security, eurograbber attack, mobile malware.

IJSER

INTRODUCTION

In a distributed organization, varieties of capital are dispersed in the structure of composite services in distributed make available and control these services by servers. Distant verification is the majority usually utilized technique to make a decision with individuality of a remote consumer. In universal, here they present are three verification aspects:

1. Impressive the customer recognizes their own password.
2. Impressive the customer has present their identity by smart card.
3. Impressive the customer with their biometric uniqueness (e.g., fingerprint, voiceprint, and iris scan).

The majority near the beginning authentication mechanism are exclusively based on password. At the same time as such protocols are comparatively simple to put into practice, secret words and person produced their own passwords in accurate have a group of vulnerabilities. By exploiting these vulnerabilities they use just use simple dictionary attacks can break these passwords in a small time. Due to these apprehensions, hardware verification signs are introduced to make strong protection to client confirmation and another is smart card supported secret code verification has develop into one of the largest part widespread confirmation methods. Smart card based password validation make available through two factor authentications, i.e. an unbeaten login wants the user have a suitable smart card and an acceptable secret code. While it makes available well-build safety measures assurances than secret code verification it could furthermore be unsuccessful if both verification issues compromised e.g., an attacker has using smart card can effectively acquired the password and their related information. In this condition, a third confirmation feature can improve difficulty and additional progress the structure's promises.

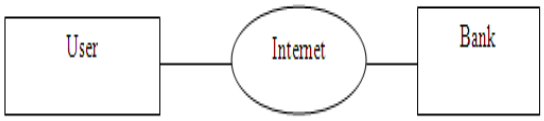

Figure 1. Traditional Security Model

Another certification method is biometric authentication [1], where clients are acknowledged by their computable human uniqueness i.e. iris scan, fingerprint and voiceprint. Biometric attributes are considered to be a consistent validation issue in view of the fact that they make available a probable resource of high entropy information and cannot be simply missing or elapsed.

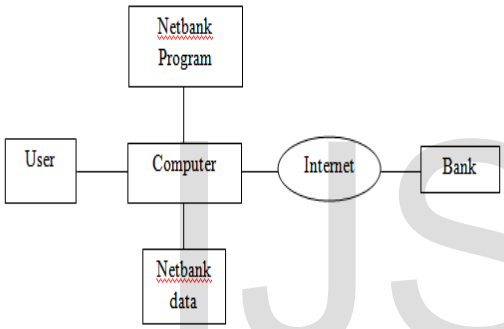

Figure 2. Revised Security Model

In spite of these advantages, biometric authentication has some disadvantage also. Unlike password, biometric characteristics cannot be easily changed or revoked. Some biometric characteristics (e.g., fingerprint) can be easily acquired without the knowledge of the owner. This leads to three-factor authentication, which incorporates the advantages of the authentication based on password, smart card, and biometrics.

Pertinent Attack Vectors and explanation Properties Research demonstrates that the final move toward as well acknowledged as "drive-by infection" increasing great attractiveness at the instance of scripting [2]. Another one is the attempt need to execute software attacks is continuously falling suitable to the aspect that the necessary information and uncomplicated to utilize instruments are accessible from the Internet at extremely small charges, consumer have troubles through maintaining their software at the most up-to-date patch level [3] Finally, software attacks are if promising at all very durable to mark out backside as the originators characteristically conceals at the back botnets and server communications hosted in a variety of distant countries and administrated by unusual authorities.

While these two attack groups alongside with appropriate verification techniques have been conversed in intensity in [4], this paper further focuses on substance exploitation show aggressions aiming the operational data penetrated by use of the user PC. This can be capable of think about the most progressed attack vector which cause to be preventative measures utilized to prevent the supplementary two attack categories such as short-time passwords created by hardware symbols or commonly legitimate SSL/TLS connections unsuccessful. Content-manipulation attacks are characteristically applied by signifies of MSW starting pointed on the user PC. Even though users protect their PCs by sustaining firewall and anti-virus software in apply MSW discovers its method to contaminate PCs by utilizing either client inadvertence or frequently come backing software insufficiency. Experience shows that it is impossible to reliably and lastingly save from harm software consecutively on today's user hardware and operating systems, lacking trusted computing support, by means of other software running on the same platform [5]. Momentarily examined success of such software be required to consequently be understood with appropriate to safety measure and as such be measured additional an effect of its proprietary environment than of any precise hardening [6]. From a continuing perception it is intelligent consequently to imagine that a client's PC that cannot be strongly rebooted for e-banking and that is frequently utilized for browsing and e-mailing over the Internet, will maintain to be representation to MSW intelligent to take in excess of complete control. Under this hypothesis an attacker does no longer could do with to appropriate confirmation documentations or crack into the protected conduit created between the client's PC and the bank's server but it will quite take undeviating advantage of MSW to without a sound present or alter transaction information at the same time as the actual customer is associated to the bank. In global instances of MSW sustaining such attack vectors are the Trojans "ZEUS", "Trojan. Silent banker" and additional attack [7]. The only extensive expression explanation to this experience become visible to come from matching

IJSER

well-built confirmation at login with susceptible data confirmation at transaction insertion and using for the extra authentication footstep a trusted stage not description to the Internet, the user PC, or any MSW potentially spreading through these means [8]. In other words, the process of confirming sensitive operation data must be progressed from the PC to an expectation piece of equipment that at smallest amount contains to show one or more buttons in addition to the user credentials. This method the client can consistently authenticate serious transaction features on the trusted demonstrate such as the beneficiary account of a payment order and then authenticate the relevant data by the use of the confidences buttons. The piece of equipment then characteristically produces a transaction precise signature to be sent to the banking server through network. Credentials utilized to do this are not at all representation to the user PC in extra remarks the trusted piece of equipment always marks what the user has seen and agreed on the equivalent machine. The primary assets of an Internet banking service presenting compensations to without restraint choose proficient recipient should be confrontation alongside the conversed attack vectors. On the other hand, also to the safety measures characteristic, other features can be regularly significant for the applicability and accomplishment of an explanation. For that reason, in this paper they as well think about the following other business appropriate explanation properties:

- **Reasonableness**: The explanation's safety measures shall be sensitive yet for a non-occurrence client i.e. dependability and appropriate carefulness are simply considerable.
- **Convenience**: The explanation shall be uncomplicated to utilize e.g. high-speed, well known interface prototypes, mobile and no software installation on user PC.
- **Mobility**: The dependences mechanism shall be uncomplicated to take approximately shall not involve software installation and shall occupation with usual PCs and operating systems.
- **Integration**: The explanation shall incorporate well with subsisting communications. This comprises client-side H/W and S/W, communication protocols, and server-side constraints.
- **Administration**: The explanation shall be straightforward to control and sustain such as by signifies of remote pattern and software update.
- **Cost**: In general asking prices shall be small to meet the constraints for far above the ground volume exploitations such as in retail banking.

Property / Solution	A	B	C	D
Connected to PC	No	No	No	Yes
Input	Manual	Auto	Auto	Auto
Output	Manual	Manual	Manual	Auto
Convenience	+	++	++	+++
Mobility	+++	+++	+++	+
Client-side Integration	+++	+++	++	+
Cost	Low	Medium	Medium	high

Table 1. Contemporary transaction authentication solutions and their properties

LITERATURE SURVEY

Xinyi Huang, Yang Xiang proposed a new and efficient technique for the privacy and security in distributed systems [9]. Here in this approach a framework has been implemented for three factor authentication. The three factor authentication implemented here using passwords and smart cards and biometric provides efficient security and authentication in distributes systems. The main aim of the paper is to provide security to the data that is being send over the wired or wireless network or in Cloud Network. The Three factor based framework on the concept of providing security using password matching and smart cards based authentication and authentication using biometric.

Thomas Weigold, Alain Hiltgen proposed a secure transaction framework for Internet Banking Services using Secure Confirmation of sensitive transaction data [10]. The paper uses an efficient technique for the security of sensitive and important data for the risk migration approach for a trusted device which can be further combined with multi-level white list management to provide

secure and authenticated transaction. The paper also implements two real world properties of providing high level of security over internet banking transactions.

Schmidt is one the person who suggested mobile malware detection for Android Smartphone [28] . This proposed algorithm derive function calls from binaries of application and for detecting unrevealed malware a clustering mechanism called Centroid is used .Which is achieved by implementing static analysis of Executable and Linking Format(ELF) objects files by utilizing command readelf in Android. The function calls and modified files which maintain those file data are compared with malwares executable for arrange them with DTL(Decision Tree Learner), Rule Inducer (RI) and), Nearest Neighbour (NN) algorithm. The author challenged that this algorithm shows up to 96% detection perfection with 10 % false positives

I.Burguera and U. Zurutuza [29] proposed a technique which dynamically analyze the behavior of Mobile(Android) Applications. For getting the traces of application behavior like system call they applied CrowDroid which is a crowd-sourcing system. In the runtime CrowDroid assemble the system calls which is used by the set of user. To classify the data in to dual group named benign group and the malicious group K-means clustering technique has been used, which can be applied to detect the end user running the infected repackaged application.

Chi Po Cheong, Chris Chatwin, Rupert Young also proposed a new and efficient technique for the security of web services using token based authentication system [11]. The existing technique implemented for the security of web services for providing message integrity and message confident ability is then improved here using an efficient and advanced technique of secure token based authentication. The new secure token based authentication implemented here provides remote client location.

Alaa Aref El Masri, Joao Pedro Sousa has provided a bounding confidential data experience for the security of online transactions [12]. The model implemented here is based on the concept of user based online privacy and assurance model. The paper mainly focuses on the facility of providing high level security for the online transaction. Here in this paper first of all elevated stage categorization of existing privacy based declaration is provided. In the next phase a detailed classification of which is support on the amount of client secrecy and the amount of transaction of traceability of transactions.

Muhammet Yildiz, Mehmet Gokturk has implemented a hybrid combination of providing authentication and security using Biometric ID certificates and online credit card based transactions [13]. The proposed system and framework is implemented on the concept of online transaction especially online shopping where all the transactions can be done using credit cards and the chances of failure of payment and loss of money is maximum. The paper solves the issues of failure of these transactions using biometric ID cards based authentication and providing security using online ID cards based authentication.

K. Nirmal, S.E. Vinodh Ewards proposed a new efficient technique for the online security and authentication using 3 Factor and measures the Counter-attacks especially phishing attack [14]. A phish-secure algorithm is implemented here which deals as Anti-phishing algorithm. It uses the concept of three factor authentication which is used for the successful detection of the unknown attacks. It is used for the identification and verification of the destination address from the packets that outbounds to the remote server. The technique implemented also reduces the time taken for the detection of phishing.
Mariano Luis T. Uymatiao, William Emmanuel S. Yu also proposed a new and efficient technique for the security and authentication of Online Transactions using Time-based OTP [15]. The paper mainly focuses on the existing cryptographic standards for the web applications depending upon multi-factor authentication cryptosystem. It uses the seed exchange for the software based tokens for the security and authentication of Transport layered security. Here time based One time password is used for the security and authentication provided in Mobile TOTP.

Marc Alexander Kowtko proposed a biometric authentication system for the older adults [16]. The paper implements an efficient and secure methodology for the security of Data using Captcha and various security questions. While username/password verification, CAPTCHA, and

security issues to make available sufficient protection; they are still vulnerable to cyber-attacks. Passwords can be cooperation from brute force, dictionary attack and social engineering approach attacks. CAPTCHA, a type of test reply analysis was increased to make certain that customer inputs were not manipulated by machine-based attacks.

Bei Guan, Yanjun Wu, Yongji Wang implemented a new and secure technique for the security of Online Banking and Transactions on Virtual Machines [17]. A using these new proposed protection method for online banking that joins the virtual machine (VM) technology with web services. Initially, DO Bank summarizes the banking service into a person of little consequence domain and save from harms it from any attacks reasoned by virus from the customer's swarm. Another way is the area can access certain hardware mechanisms entirely alongside Key logger and increases almost inhabitant presentation using exceed through expertise.

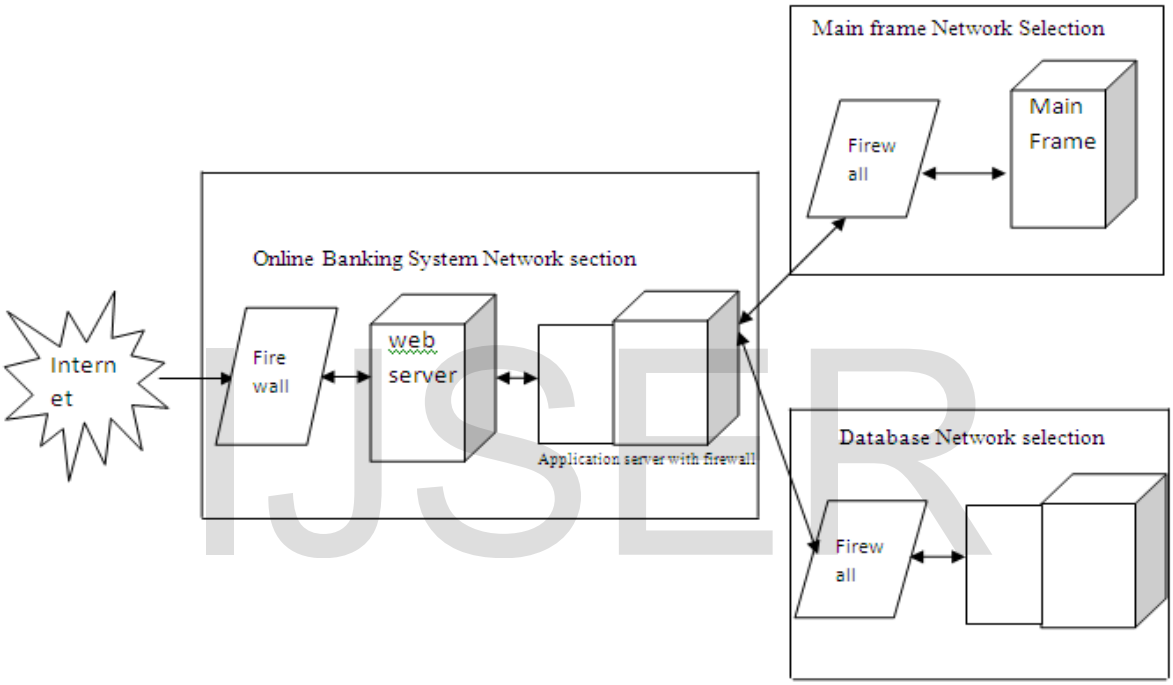

Figure 3. An Example of Chinese Server side Security System

In this paper, here author has proposed [18] a new safety algorithm that enhances the variable charges for the attacker. Attacking one client is costly but not completely impracticable for the fake. But, attacking a subsequent consumer requires approximately the complete quantity of employment on the fake another time manufacture the complete cheat too expensive for him. As a final point, they wrap up the document by conferring the safety measures suggestions of the offer circumstances which troubles can and which cannot be resolved by using our move toward.

Here in this paper author [19] has proposes a original secure token for enhancing the convectional Web Service Security ordinary which make available message reliability and message privacy. A novel protected token has been recommended for attractive the Web Service security. With the proposed indication the location of the sender can be validated which eventually decreases the command on structure stores by jamming counterfeit consumers. SOAP is a significant knowledge to put into practice SOA-based methods.

The paper [19] also shows the sentence structure of the proposed indication and the features of dealing out imperatives and stream. The benefits and constraints of the proposed indication are also conversed in the paper.

S.No.	Paper	Author	Advantages	Issues
1	Secure E-Commerce Transactions for Multicast Services [20].	Anil Kumar Venkataiahgari, J. William Atwood, Mourad Debbabi	Here multicast based authentication is provided for the secure transmission of audio/video transmission of data. It provides authentication of HIP Protocol as well as authorization of subscriber using the help of PIK.	The protocol proposed here is difficult to achieve since it requires complex framework.
2	A New Symmetric Cryptography Algorithm to Secure E-Commerce Transactions [21].	Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghigat	Here in this paper a new symmetric algorithm called FJ RC-4 algorithm is implemented which is an enhancement of RC-4. The proposed methodology implemented here is better as compared to the existing RC-4 technique	It requires lot of stages to perform hence it takes more computational time.
3.	A Solution of mobile E-Commerce Security Problems [22].	Suzhen Wang, Lijie Fan	The methodology implemented here is the enhancement of WAP gateway. The vulnerable point is first analyzed and then applying double encryption model to provide security in WAP gateway. The methodology implemented here reduces the communication cost as well as increases the connection speed and security of mobile based transactions.	The methodology is not feasible for all types of mobile frameworks.
4.	Met: Multi party E-Commerce Transaction Model [23].	Keren Jin, Jiafeng Zhu, Guangbin Fan.	A new model for the multi party based E-Commerce transaction is proposed which provides efficient security from various attacks in the E-Commerce applications. The methodology provides authorization from various attacks on the basis of transactions from various users/parties.	Requires authorization and authentication from various parties hence requires more computational time.
5.	Efficiently Achieving Full Three-Way Non Repudiation in	Stephen W. Neville, Michael Horie.	Here in the paper a new and efficient protocol is implemented which is	Chances of latency is increased as well as overhead.

IJSER

	Consumer-level E-Commerce and M-Commerce Transactions [24].		fruitful for E-Commerce and M-Commerce applications and transactions. A secure and efficient (<5 seconds) consumer-level E-Commerce as well as M-Commerce protocol is implemented which provides non-repudiation and security from various attacks possible in E-Commerce/M-Commerce Transactions.	
6.	E-Commerce Security Through Asymmetric Key Algorithm [25].	Ankur Chaudhary, Khaleel Ahmad, M.A. Rizvi.	Here in the paper a new and efficient PGP based protocol is implemented which provides more security in case of online transaction based on dual signatures. The proposed algorithm here is Asymmetric which provides more security and takes less computational cost.	The proposed algorithm implemented here requires less security from various attacks.
7.	A Model to Secure E-Commerce Transaction using Hybrid Encryption [26].	Devendra Singh Solanki, Dr. Savita Shiwani.	Hybrid cryptography is implemented here by combining the advantages of both symmetric and Asymmetric cryptography to make offered secure transaction in E-Commerce applications.	The methodology implemented is not feasible since the chances of attack increases because of anomalous behavior.
8.	ReputationPro: The Efficient Approaches to Contextual Transaction trust Computation in E-Commerce Environments [27].	Haibin Zhang, Yan Wang, Xiuzheng Zhang.	Here in the article a trust vector is implemented to provide contextual transaction trust. In the computation of CTT charges, three identified crucial context dimensions, including Product Category, Transaction quantity, and Transaction Time are in use into clarification. In the meantime, the computation of each CTT value is based on both earliest time's transactions and the move about in the direction of transaction.	For the improvement of the methodology a deletion operation is added in CMM-tree for better performance.

IJSER

CONCLUSION

Here various Security algorithms implemented for the Online Transactions is analyzed and discuss their various advantages and limitations. There are various methodologies in which the prior concern is security from various attacks during online Transactions. Some techniques involve working on Computation such as Communication cost and Storage and Computational Time. By Analyzing the various techniques implemented for Online Transactions it is found that the work implemented so far may contains some issues in the methodologies which needs to be solved in future by applying some improved technique which not only provides security from various attacks but also provides efficient improvement in Computation.

REFERENCES

[1] Ed. Dawson, J. Lopez, J.A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure," Proc. IEEE Int'l Conf. Information Technology: Research and Education (ITRE '03), pp. 274-278, 2004.

[2] Reporting and Analysis Center for Information Assurance (MELANI), "Information Assurance – The Situation in Switzerland and internationally", Semi-annual report (public), http://www.melani.admin.ch/dokumentation/00123/00124/index .html?lang=en (Access date 24 November 2010).

[3] Stefan Frei, Thomas Duebendorfer, Bernhard Plattner, "Firefox (In) security update dynamics exposed", ACM SIGCOMM Computer Communication Review, vol. 39, issue 1, January 2009, pp. 16-22.

[4] A. Hiltgen, T. Kramp, T. Weigold, "Secure Internet Banking Authentication", IEEE Security and Privacy Journal, vol. 4, no. 2, March/April, 2006, pp. 21-29

[5] D. Challener et. al., "A Practical Guide to Trusted Computing", Prentice Hall Computing, 2007, ISBN 978 0132398428.

[6] C. Ronchi, S. Zakhidov, "Hardened Client Platforms for Secure Internet Browsing", in N. Pohlmann, H. Reiner, W. Schneider (Editors): Secure
Electronic Business Processes, Vieweg (2008), pp. 367-379..

[7] U. Nattakant, "Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Customers", Proc. 7th Australian Information Security Management Conference, 2009, paper 19, http://ro.ecu.edu.au/ism/19 (Access date 24 November 2010).

[8] R. Oppliger, R. Rytz, T. Holderegger, "Internet Banking: Client-Side Attacks and Protection Mechanisms", IEEE Computer, vol. 42, no. 6, June 2009, pp. 27-33.

[9] Xinyi Huang, Yang Xiang, Jianying Zhou and Robert H. Deng," A Generic Framework for Three-Factor Authentication; Preserving Security and Privacy in Distributed Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 8, August 2011.

[10] Thomas Weigold, Alain Hiltgen," Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services", IEEE 2011.

[11] Chi Po Cheong, Chris Chatwin, Rupert Young," A New Secure Token for Enhancing Web Service Security", IEEE 2011.

[12] Alaa Aref El Masri, Joao Pedro Sousa," Limiting private data Exposure in Online Transaction", 2009 International Conference on Computational Science & Engineering", IEEE, Vancouver, BC, 2009.

[13]Muhammet Yildiz, Mehmet Gokturk," Combining Biometric ID Cards and Online Credit Card Transactions", 2010 Fourth International Conference on Digital Society", IEEE 2010.

[14] K. Nirmal, S.E. Vinodh Ewards," Maximizing Online Security by providing a 3 Factor Authentication System to Counter-attack Phishing", IEEE 2010.

[15] Mariano Luis T. Uymatiao, William Emmanuel S. Yu," Time-based OTP Authentication via Secure Tunnel (TOAST): A Mobile TOTP Scheme using TLS Seed Exchange and Encrypted Offline Keystore", IEEE 2014.

[16] Marc Alexander Kowtko," Biometric Authentication for Older Adults", IEEE 2014.

[17] Bei Guan, Yanjun Wu, Yongji Wang," A Novel Security Scheme for Online Banking Based on Virtual Machine", 2012 IEEE Sixth International Conference on Software Security and Reliability Companion, IEEE 2012.

[18] Martin Boesgaard and Erik Zenner, "Protecting Online Transactions with Unique Embedded Key Generators Second International Conference on Availability, Reliability and Security (ARES'07) 0-7695-2775-2/07 2007.

[19] Chi Po Cheong, Chris Chatwin, Rupert Young, "A New Secure Token For Enhancing Web Service Security" 978-1-4244-8728-8/11/ IEEE 2011.

[20] Anil Kumar Venkataiahgari, J. William Atwood, Mourad Debbabi," Secure E-Commerce Transactions for Multicast Services", Proceedings of the 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), IEEE 2006.

[21] Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghighat," A New Symmetric Cryptography Algorithm to Secure E-Commerce Transactions", 2010 International Conference on Financial Theory and Engineering, IEEE 2010.

[22] Suzhen Wang, Lijie Fan," A solution of mobile e-commerce security problems", 2010 2nd International Conference on Education

Technology and Computer (ICETC), IEEE 2010.

[23] Keren Jin, Zhu Guangbin Fan," MET: Multi party E-Commerce Transaction Model", 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, IEEE, Boston MA, 2011.

[24] Stephen W. Neville, Michael Horie," Efficiently Achieving Full Three-Way Non-repudiation in Consumer level eCommerce and M-Commerce Transactions", 2011 International Joint Conference of IEEE TrustCom 11/IEEE ICESS-11/FCST-11, IEEE 2011.

[25] Ankur Chaudhary, Khaleel Ahmad, M.A. Rizvi," E-commerce Security Through Asymmetric Key Algorithm", 2014 Fourth International Conference on Communication Systems and Network Technologies, IEEE 2014.

[26] Devendra Singh Solanki, Dr. Savita Shiwani," A Model to Secure E-Commerce Transaction using Hybrid Encryption", 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCI)", IEEE 2014.

[27] Haibin Zhang, Yan Wang, Xiuzheng Zhang,," ReputationPro: The Efficient Approaches to Contextual Transaction Trust Computation in E-Commerce Environments", ACM Transactions on the Web, Vol. 9, No. 1, Article 2, Publication date: January 2015.

[28] D. Damopoulos, G. Kambourakis, S. Gritzalis, and S. O. Park, "Exposing mobile malware from the inside (or what is your mobile app really doing?)," Peer-to-Peer Netw. Appl., Dec. 2012.

[29] I. Burguera and U. Zurutuza, "Crowdroid : Behavior- Based Malware Detection System for Android," Proc. 1st ACM Work. Secur. Priv. smartphones Mob. devices (SPSM '11), 2011

.

IJSER