E-commerce security issues and consumers' attitudes - a perspective

Lingaraj A Hadimani[1]
Dept.of Electronic and Computer Engineering,
Caledonian College of Engineering,
Muscat, Sultanate of Oman,
E-mail: lingaraj@caledonian.edu.om

M G Shinde[2]
Dept. of Electronics and Telecommunication,
MET's Institute of Engineering,
Bhujbal Knowledge City, Nashik Maharashtra India
E-mail: manisha.shinde1@gmail.com

R G Dabhade[3]
Dept of Electronics and Telecommunication Engineering,
SND College of Engineering and Research Center,
Yeola, Dist: Nashik, Mahasrahtra India
Email:rgdabhade@gmail.com

S V Khandge[4]
Department of Computer Science & Engineering,
BV College of Engineering and Research Center
Nashik, Maharashtra India
E-mail: sandhyav.khandage@gmail.com

Abstract - **The Sultanate of Oman is witnessing tremendous increase in the usage of internet during past few years. Especially, the growth of the banking industry in Oman is due to the strong economic performance, liberalization of the economy, diversification, major infrastructure developments and accelerated privatization program. This combined growth lead to a considerable increase in E - commerce activities. However, there are growing concerns among the customers of various business sectors about the safety and security of their private information. Therefore, online security is one of the most important issues in building the confidence among online consumers. Hence, this research aims to investigate the awareness about the security issues related to e-commerce and to analyze the effect of concern on the quantum of transactions carried out. This research uses deductive approach and mainly taken in Muscat, the capital of Sultanate of Oman. The research methodology consists of collection of information through questionnaires, group discussion and focus group interview. The results of the research work indicate that access control, authentication, confidentiality and lack of the awareness of security systems are the major security issues that affect consumers' attitudes. The demand for educational and awareness programs are recommended in order to contribute and increase the use of online transaction in the Sultanate.**

Keywords- E-Commerce, access control, authentication, confidentiality, ITA, E-enabled services.

I. INTRODUCTION

The basic requirement of the consumers to undertake online transaction is the knowledge about internet usage and some basic security issues. According to the available current statistics from Ministry of National Economy, Sultanate of Oman, the number of Internet subscribers in Oman are 101,890 and this represent about 3.7% from the total population of Oman [14]. There are no actual statistics which describe the number of consumers using E-commerce or any other online services. But it is sure that not all the subscribers are using Ecommerce due to lower income, lack of awareness or security issues etc.

To enforce the government policy and regulations in implementing e-governance in the Sultanate, Information Technology Authority of Oman (ITA) is encouraging consumers to make use of the online transaction facilities wherever possible. But even after substantial efforts, people are reticent to use online transaction in E-Commerce activities. [5]. Doubts are raised on certain factors such as lack of knowledge and skills of using computer, lack of confidence and trust, difficulties in accessing internet service, lower marketing or lack of knowledge in E-commerce security issues. This study focused on some E-commerce security issues such as privacy, identification and authentication, access control, data confidentiality, data integrity and non-repudiation. Also, the effect of these factors on the consumers' is analyzed.

II. LITERATURE REVIEW

Effective use of Ecommerce activities can help the economies of developing countries. The greatest and the most benefit of Ecommerce is that it empowers even small business enterprises or an individual to reach the global market. Despite the huge numbers of internet users, still the willingness of consumers to go for the online shopping is low and this is due to lack of trust [7]. A study conducted shows that consumers' are not trusting the online vendors [17]. Several studies emphasized that consumers' don't trust online security methods, despite the use of encrypted information by using protocols such as Secure Sockets Layer (SSL) or Secure Electronic Transactions (SET) which are very secure and not easily breakable [3],[2],[8].

The illegal activities of hackers are the concerns for online consumers. They can filch the credit card details which are transmitted over the internet. A survey of consumers' attitudes towards the internet found that 89% of experienced consumers' are concerned over the use of credit cards while transacting online and this increased to 98.6% for new consumers. The critical information that is transmitted over the network can be obtained by using software programs called packet sniffers. Moreover, attackers will hardly use this complicated and long procedure to collect few credit card numbers. A number of websites provide easy access to database containing all the important information of their customers' accounts. Therefore, it is very important to secure the Ecommerce firm's websites before securing the online transactions [21].

It is also felt that there is a need of strong protection to companies' website's and databases as they are more vulnerable to the attacks [13]. And this could be achieved by implementing security management systems which will define the way of using internet. The next step is to identify the possible threats like data destruction or unauthorized disclosure and manage them with convenient means [13]. In contrast some researchers have the opinion that security is not a prime concern but as day by day penetrations are increasing there is a need for having a strong protection and security measures to the critical data.

Usually, consumers provide information to online vendors for verifying identification and authentication. Online merchant's system could use monitoring programs for providing protection against theft. These programs surreptitiously will allow online firms to use consumers' personal information and sell it to others. And the consumers are really concerned about these kinds of unethical issues as they lose very important personal information. Many of the research works have addressed regarding the types of privacy concerns identified by the online consumers. It may be a small privacy concern such as nuisance from a junk mail or a big online transaction which involves huge financial information. Vendor's actions sometimes cause improper use of consumer's personal information [16].

Another study which mainly focused on online consumers' behaviors and their decision to buy or not to buy showed that convenience and good customer services are the key factors for online business [1]. There is a need to have awareness programs related to security issues and these programs could overcome or minimize the gaps in lack of security awareness to consumers [6].

A framework was developed considering the key driving global forces as primary source and national policy forces as enablers to the growth of e-business in the Asia-Pacific region [9].

III. RESEARCH METHODOLOGY

The research philosophy deals with the way of thinking in the process of knowledge development. There are three philosophies in the research process: Positivism, Interpretivism and Realism [18]. This research uses positivism to measure the consumers' attitudes towards E-Commerce security.

However, making a decision in selecting the correct research approach is very important [4]. This depends on clarity of theory adopted at the beginning of the research. There are two main research approaches which are known as deductive and inductive. The deductive approach tests a theory whereas in an inductive approach, collection and analysis of data is done before building or developing a theory [18]. This study uses deductive approach, which deduces a hypothesis from theory and tests the hypothesis also. It also examines the findings and if necessary, modifies the theory based on the research outcomes.

As a theoretical basis, a model is proposed (Fig.1) for discussion and analysis. The model has been tested and used together with with the findings of questionnaire. The proposed model is grouped into two main categories. The first category is security issues influencing consumers' attitudes in the security management system and the second contains issues which are influencing consumers' attitudes in transaction system at online environment.

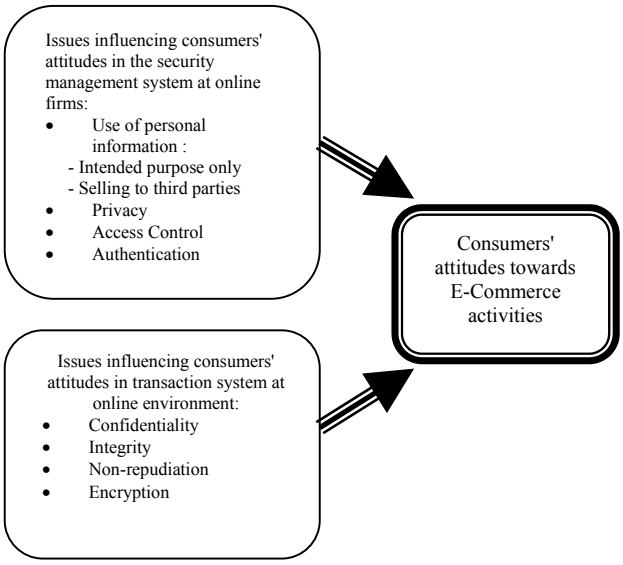


Fig.1 Research proposed model

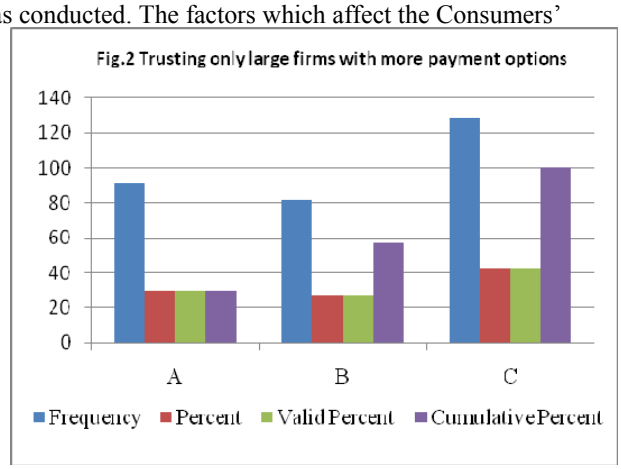
A survey is used in this study as a research strategy. It is a collection of information in a standardized form from selected samples of populations. It used for creating quantifiable data.

The research uses a mixed method of quantitative and qualitative approach. The benefit of using a mixed method is that, it lets the researcher to validate hypothesis and a conceptual model to obtain a better understanding of results [15]. In addition, the findings from a qualitative study can be used to explain and confirm the results which are collected from the quantitative study [12].

The Quantitative method has been used for testing and validating the research hypotheses with the proposed model. Therefore, the questionnaire was designed as a research tool for collecting information. It also can be used an appropriate tool for measuring attitudes or opinions. In addition to this, a focus group interview of 6-12 people was conducted for confirming the findings from the survey. This qualitative method provides the researcher to deeply explore attitudes, beliefs and reaction of consumers. Moreover, it may not be viable with some data collection methods. The important issue in a focus group is that the research topic can be more focused and explored in friendly atmosphere with an open discussion and interaction between participants [10]. Therefore, it is also an appropriate method for extracting consumers' attitudes.

According literature, a survey method has two important elements known as randomization and bias. This method requires the researcher to select samples from the general population that will be statistically and logically defensible [11]. Samples are narrowed from the population of (2, 743000) in the Sultanate to a more focused segment of (101,890) number of Internet subscribers in Oman [14].

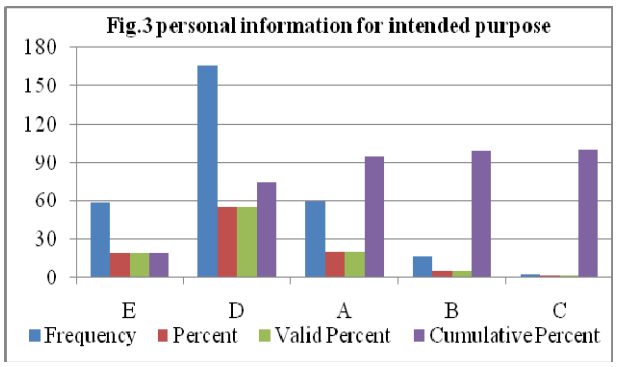
After collecting the data, Statistical Package for Social Sciences (SPSS version 16.0) software is used for analyzing the results. It codes the data for generating a descriptive statistical analysis such as frequencies, means and standard deviations. For achieving more reliability to the questionnaire, Cronbach's alpha test of reliability correlation was conducted. The factors which affect the Consumers' attitudes towards Ecommerce security were identified by performing factor analysis. Moreover, the proposed model with hypothesis was tested with Pearson correlation coefficients which test the relationship between influencing factors and consumers' attitudes towards security in e-Commerce.



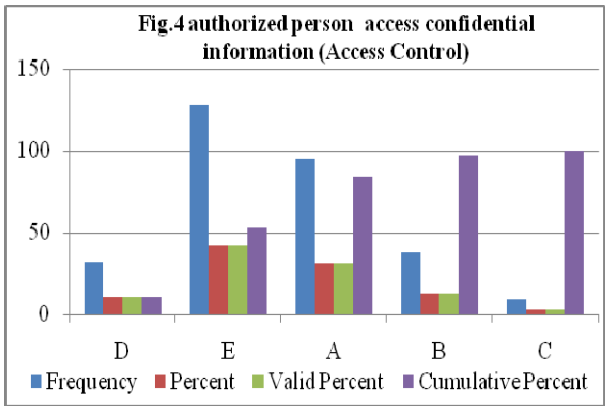
IV. RESEARCH FINDINGS

A. Questionnaire Findings

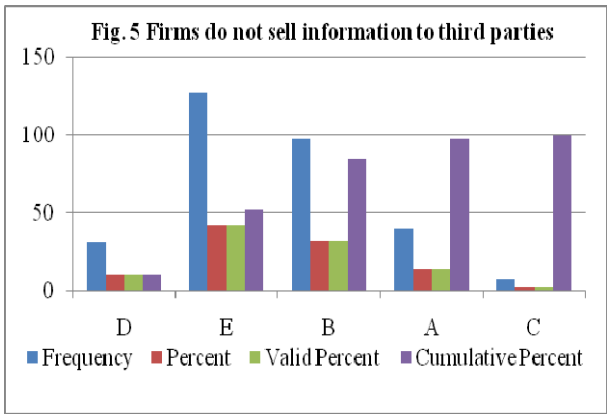
The questionnaire was circulated in Muscat governorate based on sample size of 384. In addition to the delivery and collectable self-administered questionnaire, online questionnaire was also distributed among the customers who work in different organizations. Questions were based on the customers' attitudes towards the security management systems which are adopted by online firms. The questions were aimed to evaluate the respondents' opinion. In addition to the questions, a brief was also included about trusting the online firm's systems as most of them protect consumers' personal information. The results of the survey are plotted from Fig.2 to 7 (A=neither agree nor disagree, B=Agree, C = strongly agree, D=strongly disagree, E = Disagree)



Around 70% of respondents stated that they would trust only large firms which have more payment options. Out of 302 responses, there were only 18 respondents (about 6%) who believe that the online firms will not use their personal information for any purpose unless they authorized them.



More than 74% do not believe that firms use personal information for intended purpose only. Others indicated that they are not sure about this statement. Fig.4 shows, less than 17% of respondents agree that only authorized person can access confidential information in firm's system. About 31.5% of respondents were neither agree nor disagree (neutral). It is clear that the majority of respondents disagree about this statement. More than 52% of respondents do believe that firms may sell their personal information to the third parties whereas only 15.5% of respondents trust that firms do not sell information. The remaining (32.1%) stayed neutral in their opinion. More than 79% of respondents have considered the authentication is an important concern.

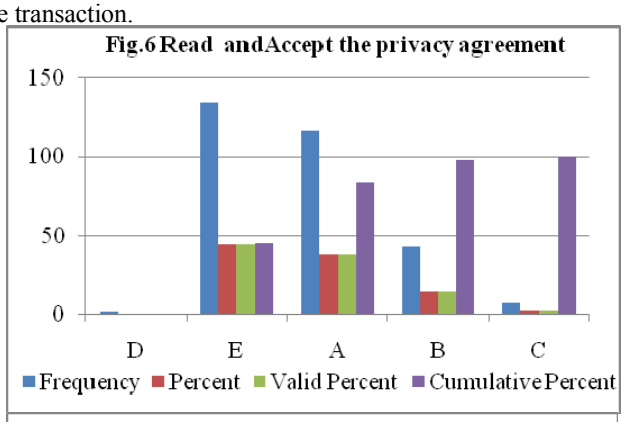


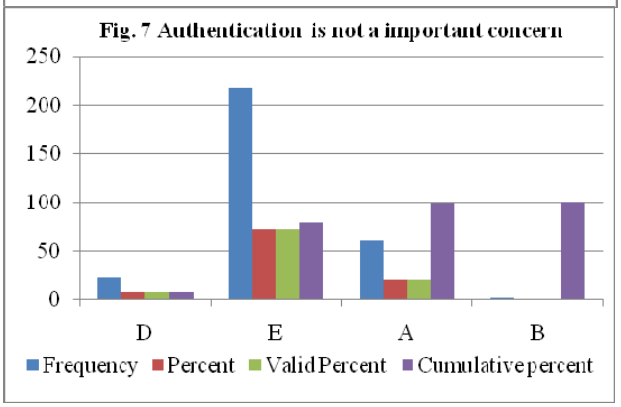
Most of respondents do not show interest in reading and accepting the privacy agreement. Only about 16.5% of them have read the consumers' privacy agreement. More than 79% of respondents have considered authentication as an

important concern. Most of respondents do not show interest in reading and accepting the privacy agreement. Only about 16.5% of them have read the consumers' privacy agreement.

B. *Focus Group Findings*

All the participants were aware of the credit card misuse and misappropriation by the media. They believe that online firms will sell their important personal and financial information to the third parties. They strongly disagreed that online firms use their information for the intended use only. Most participants were not aware about consumer's privacy agreements. Many of them agreed that, data accessibility is an important factor. However, they were not sure that only an authorized person can access the confidential information. They also stated that authentication is a crucial factor, which protects their personal information. They were really concerned about the safety of the information they provide to the online firms. Except one participant, all of them were not aware of the fact that the data can be altered during the transaction. Most of the participants were reluctant to believe that the online firms or third parties can not alter and deny the transaction.





V. RESULT ANALYSIS

Factor analysis was conducted to find the variables which are correlated to each other. The relationship between Consumers' Ecommerce activities and Security issues were analyzed by using the principal components method of extractions. The rotated component matrix method helped to determine what exactly each component represented. The first component was most highly correlated with selling information to third parties. The second component had high correlation with confidentiality and the third component with authentication.

Table 1: Results of Rotated Component Matrix

Rotated Component Matrix			
Factors affecting Consumers	Component		
	1	2	3
Conducting E-Commerce activities	-.337	-.050	.794
Firms use personal information for intended purpose only	.758	.173	-.022
Only authorized person can access information	.902	-.102	-.018
Firms sell information to third parties	.907	-.045	-.111
Attention to read and acceptance the privacy agreement	.815	.102	.050
Authentication is not important concerns	.165	.104	.827
The payment information is confidential and not accessible	.038	.860	-.131
The financial information is encrypted	.603	.497	-.022
The financial information do not alter through the route	.738	.417	-.116
Both parties cannot deny the confirmed transaction	.069	.735	.353
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			
a. Rotation converged in 4 iterations.			

However, Component Score Coefficient Matrix method produced more better and accurate results. The component score is calculated by multiplying the case's standardized variable values with the component's score coefficients. The first component has got the highest correlation with Access Control (0.273). Whereas, firms do not sell information factor was the highest in rotated component matrix method. The second and third components have highly correlated with Confidentiality (0.553) and Authentication (0.579), which is also true with earlier method. Therefore, according to factor analysis these components represent the most important issues that affect Muscat consumers' attitudes towards conducting E-Commerce activities.

VI. CONCLUSIONS

In the near future, E-commerce may play a major role in everybody's life as people are not finding time to go to the shopping centers to buy the products in their busy schedules. Moreover, advances in Internet technology are prompting the users to adopt the Ecommerce business. In this scenario, it is important to adopt some strong security measures to prevent

online crimes or thefts so that more number of customers should get attracted towards online Shopping. Also, there is a

Component Score Coefficient Matrix			
Factors affecting Consumers	Component		
	1	2	3
Conducting E-Commerce activities	-.033	-.056	.533
Firms use personal information for intended purpose only	.193	.008	.024
Only authorized person can access information	.273	-.187	.062
Firms sell information to third parties	.260	-.143	-.008
Attention to read and acceptance the privacy agreement	.224	-.051	.084
Authentication is not important concerns	.093	-.030	.579
The payment information is confidential and not accessible	-.117	.553	-.165
The financial information is encrypted	.104	.235	-.016
The financial information do not alter through the route	.147	.174	-.065
Both parties cannot deny the confirmed transaction	-.056	.427	.186
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			

Table 2: Results of component score method

strong need of security related awareness among the customer base for the safety of the information they provide. Building trust on Ecommerce among the customers is a great challenge as today's media publicizes every single fraud which takes place in any kind of transaction.

This research work primarily aimed to investigate the impact of security issues on the consumers' behavior towards online business. The secondary aim was to measure the customers' awareness towards security related issues.

During this research, we found that most of the people are still not aware about the type of information they require for the online transaction. Many of them are hindering to Ecommerce as they think it is very tedious and complex process. This shows that there is a strong need of awareness programme in Sultanate of Oman, which enable the customers for effective and frequent use of online business.

The people who are already aware about the security issues are also often not using online transactions because of lack of trust. The analyses of all the results show that lack of awareness in security issues is the prime concern for not trusting the online business environment. Factor analysis indicated that, Authentication, Confidentiality and Access Control were the major security issues that affected consumers' attitudes.

REFERENCES

[1] Ahuja, M., Gupta, B. and Raman, P. (2003) 'An empirical investigation of online consumer purchasing behaviour', Communications of the ACM, Vol. 46, No. 12, pp.145–151.

[2] Archetype/Sapient. (1999), eCommerce Trust Study, Cheskin Research and Studio, January.

[3] Berlin, M. (2000), "Global Online Retailing", *Ernest and Youn*g, 1(2), 1-165.

[4] Creswell, J.W. (2003) Research Design: Qualitative, Quantitative and Mixed Method Approaches.California: SAGE Publications, Thousand Oaks.

[5] Digital Oman. (2006) 'Thoughts on e-government, the economy, e-commerce and broadband', 1-on-1, issue6, p11.

[6] Furnell, S.M. and Kareweni, T. (1999).'Security implications of electronic commerce: a survey of consumers and businesses', Electronic Networking Applications and Policy, Vol.9, No.5, pp.372-382.

[7] Hoffman, D.L., Novak, T.P. &Peralta, M. (1999), Building consumers trust online, Communications of the ACM, Vol.42, pp.80-85.

[8] Jarvenpaa, S.and Todd, P.A. (2000), "Is there a future for e-retailing on the Internet?" Electronic Marketing and the Consumer, pp.139-154.

[9] Javalgi, R.G., Wickramasinghe, N., Scherer, R.F. and Sharma, S.K. (2005) 'An assessment and strategic guidelines for developing e-commerce in the Asia-Pacific region', International Journal of Management, Vol. 22, No. 4, pp.523–531.

[10] Krueger, R A, & Casey, M A 2000, Focus groups: a practical guide for applied research, 3rd edn, Sage Publications, Inc.

[11] Leedy, P. D. (1997) Practical Research: Planning and Design, Prentice-Hall, New Jersey.

[12] Maxwell, J A, & Loomis, D M 2003, 'Mixed methods design: an alternative approach', in A. Tashakkori & C. Teddlie (eds), Handbook of mixed methods in social & behavioral research, Sage Publications, London, pp. 241–271.

[13] McGuire, Brain L., and sherry N. Roser (2000). What Business should know about Internet Security, Strategic Finance, Vol.82, No.5, pp 50-54.

[14] Ministry of National Economy (MONE)-Oman. (2009). Major economic & social indicators [online]. Available from: http://www.mone.gov.om/book/mb/feb2009/T1.pdf [Accessed 1 March 2009].

[15] Newman, I, Ridenour, C S, Newman, C, & DeMarco, G M P, Jr. 2003, 'A typology of research proposes and its relationship to mixed methods', in A. Tashakkori & C.

[16] Pavlou, P. A., Liang, H. & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: a Principal-Agent Perspective. MIS Quarterly, 31 (1), 105-136.

[17] Salam, A.F., Rao, H.R. and Pegels, C.C. (2003) 'Consumer-perceived risk in e-commerce transactions', *Communications of the AC*M, Vol. 46, No. 12, pp.325–331.

[18] Saunders, M., Lewis, P. & Thornhill, A. (2007). Research Methods for Business Student.4th ed. Harlow: Pearson Education.

[19] Sipior, J.C., Ward, B.T. and Rongione, N.M. (2004) 'Ethics of collecting and using consumer internet data', Information Systems Management, Vol. 21, No. 1, pp.58–66.