Review of Privacy Issues Associated with Mobile Commerce Based Applications

Ramakala Ramaraj[#1], Rajalakshmi Subramaniam [##2],

Abstract— New innovations in the digital technology have encouraged the progress of mobile commerce markets all over the globe. Purpose of this paper is to review various privacy issues associated with mobile commerce based applications. Privacy issues which are taken into consideration are misuse of data, lack of trust, identity theft and lack of transparency. These issues are reviewed through systematic review of prior literature. This research makes use of secondary handled data from various prior sources such as journals, company's publications, books and more. It was suggested that service providers of mobile commerce have to concentrate on the issues related with privacy in order to attract existing customers as well as to acquire new customers. It is clear that rectifying these privacy issues related to mobile commerce like misuse of data, identity theft and lack of transparency can enhance the trust level among customers towards adopting mobile commerce. All privacy issues associated with m-commerce based applications cannot be given permanent resolution but can be prevented and avoided to certain extent. Future work can be expanded by other investigators in a quantitative way of approach through primary source of investigation to examine about the privacy issues associated with the mobile commerce based applications

Index Terms—.mobile commerce, privacy issues, lack of transparency, lack of trust, misuse of data, identity theft and trust

1 INTRODUCTION

Communication and information technologies are growing daily. Outcomes of advanced communication and information technologies are mobile devices. With the adoption of latest technologies mobile commerce or m-commerce has changed as a part of routine life. M-commerce make sure to give information anytime and anywhere. It maximizes the communication between consumer and business as well as make it simpler as such internet. Base of m-commerce is the internet. Industries of market research show huge chances for mobile services which would change the activities of customer from electronic decade to mobile decade [1]. With the introduction of mobile and wireless technologies, a novel signal of commerce driven based on technology has initiated namely m-commerce all over the globe. The word 'mobile' denotes to applications which are designed for customers on the mobile that is users are not dependent of application due to their location. It refers that all wireless application do not belong to mobile application [2][3].

Characteristics of m-commerce have some unique features which provide with some benefits against traditional commercial transactions form encompassing electronic commerce namely ubiquity, immediacy, pro-active functionality, localization, instant connectivity, simple authentication procedure [4][5]. Mobile application is an extension of more conventional application of user computer [6][7]. M-commerce characteristics which create value are recognized based on 5 classification requirements such as efficiency, time critical, mobility related needs, entertainment and spontaneous [8]. It has developed itself a novel place in the business transaction field, being a more convenient to adopt and cheaper alternative than an electronic commerce as pointed out by Qingfei [9].

[#]Project Handler, Talaash Research Consultants, Chennai

[##] Chief Executive Officer, Talaash Research Consultants, Chennai

[1] projecthandler2@talaash.co

[2]admin@talaash.co

Table 1: Classes of M-commerce applications

M-commerce applications	Examples of services offered
Mobile banking	• Mobile accounting • Mobile brokerage • Mobile financial information
Mobile entertainment	• Mobile gaming • Download of music and ring tones • Download of videos and digital images • Location-based entertainment services
Mobile information services	• Current affairs (financial, sport and other news) • Travel information • Tracking services (persons and objects) • Mobile search engines and directories Mobile office
Mobile shopping	Mobile purchasing of goods and services
Mobile marketing	• Mobile couponing • Direct (context-sensitive) marketing • Organization of mobile events • Mobile newsletters
Mobile ticketing	• Public transport • Sports and cultural events • Air and rail traffic • Mobile parking
Telematics services	• Remote diagnosis and maintenance of vehicles • Navigation services • Vehicle tracking and theft protection • Emergency services

Table 1 explains the classes of m-commerce applications. Services offered by the mobile banking are mobile brokerage, mobile financial information and mobile accounting. Services offered by mobile entertainment are mobile gaming, entertainment services based on location, download of videos, ring tones, music and digital image. Services offered by mobile information systems are travel information, current affairs (sport, financial and other news), tracking services, directories mobile office and mobile search engines. Services offered by mobile marketing are direct marketing, mobile couponing, mobile newsletters and organizing mobile events. Services offered by mobile shopping are mobile purchasing of goods and services. Services offered by telematics services are navigation services, tracking the vehicle and theft protection, vehicle's remote diagnosis and protection, emergency services. Services offered by mobile ticketing are mobile parking, sports and cultural events, public transport and air and rail traffic [10].

The aim of the research is to review various privacy issues associated with mobile commerce based applications. Privacy issues which are taken into consideration are misuse of data, lack of trust, identity theft and lack of transparency through systematic review of prior literature

2 Literature Review

2.1 Misuse of data:

Various investigators acknowledged that misuse of data [11] [12] [13] [14] [15] [16] [17] would develop severe privacy concerns. Culnan and Armstrong [18] argued that customers face 2 types of privacy issues. 1st, they are worried about illegal access to personal information due to shortage of internal controls or security breaches. 2ndly, consumers are worried about threat of secondary use that is again using their personal information for other uses without their permission. It combines the transaction data of customers and other personal information for creating a profile. The research of employee privacy has given a sensible base for understanding the basis of privacy as a concept of personal control as illustrated by Webster and Zweig [19] [20]. Loss of control over data that is misuse of data is vital to the idea of privacy invasion [17]. Issues about security, confidentiality and privacy are often asked by customers in term of wireless technology particularly with respect to the access of personal data and area of control [21] [22]. Further, from the customer point of view, privacy is viewed as the control over providing the personal data [23] [24].

Customer perceived uncertainty and higher risks like misuse of personal and financial information and loss of data would discourage them in adopting services of mobile banking as explained by various researchers [25][26][27][28]. Faster development in technology of mobile computing not only develops some chances for business and also poses severe issues such as misuse of data and technology [29]

Satariano and MacMillan [30] identified that Apple and Google, the top players of the mobile industry were often hindered by issues of security and privacy which arise from 3rd party developers for application and they try to utilize their operating systems for illegal profit. Even though these leaders in the market put more effort on fighting such misuse, issue is far away from acquiring permanent solution. At the same time, Niranjanamurthy et al [31] stated that payment details given by the customers will be misused by the fraudulent vendors in the m-commerce. For that, customers are worried about giving more personal information. Such activities develop a condition of unauthorized or misused disclosure [16]. On the other hand Abdul and Mohamed [32] have stated that from information system point of view, privacy of information is very significant for protecting customers from turning into victim towards changing information, unauthorized access and misuse of data by other parties.

Gao and Kupper [33] suggested that radio frequency identification, barcodes and positioning are key technologies adopted to make communication easier between mobile consumers and applications systems of m-commerce to develop new advertisement and interaction patterns and for serving customers. Such technologies can acquire acceptance if consumers' priva-

cy is not violated based on the data given by them that is misuse of data should be violated.

2.2 Lack of trust:

Numerous researchers and investigators have proved that lack of trust [34] [35] [36] [37] [38] [39] [40] and it is one of main obstacle among privacy issues faced by users in adopting the mobile commerce technology [41] [42] [43] [44] [45] [46]. Some scholars claim that at least in mobile payments consumer trust has to be developed [47] [48]. Fake usage occurs due to illegal transaction that minimizes the trust level among customers of mobile banking [49].

Some investigators have found privacy and security are 2 main fundamentals for online trust [50][51][52]. Abdul and Mohamed [32] added that personal information has to be controlled than disclosing such information for gaining customers trust. There are various reasons which cause risks when people develop trust. Associations of various forms involve noticeably unique risks since factor related to risk differs uniquely as the relationship form differs. Apart from these, risky factors also occur in matters and circumstances located by people. Therefore, service providers have to focus on developing trust among customers. Similar to that, Harris [51] added that trust plays a main role in adoption of m-commerce among users. Brown and Muchira [53] found that lack of trust cause customer to face privacy issues. Addressing such issues would be critical to develop ultimate and stable profitable relationship among customer.

Various investigators have identified that [54] [55] [56] [57] lack of trust as a main factor which affects the uptake of services in m-commerce. Trust is important in some cases which are found to be risky, and mobile commerce shows new risks and vulnerabilities to the users. It is complicated to develop trust in mobile commerce although it is a main element for the adoption of m-commerce [58]. In spite of the value of m-commerce in small and medium sized tourism enterprises, trust is one of the main hurdles in adopting the technology of m-commerce as illustrated by Joubert and Belle [59]. For becoming viable m-commerce has to overcome the trust issues among users [47]. Lack of data security and sharing of data would result in loss of consumer trust towards services system of m-commerce as mentioned by Tarasewich [60]. Hillman et al [61] identified that level of trust among customer decreases due to loss of money in the m-commerce activities.

Rehman and Coughlan [62] pointed out that personal digital assistants and smart phone users all over the globe were facing complexities to become trustworthy and accustomed in m-commerce. Major reason behind it was lack of trust and slow variation in systems of mobile payment. Author also provided best probable solution based on principles of human computer interaction. On the other hand, it was stated that lack of trust and fear of privacy issues encompassing fear of losing personal data, lack of proper standards for safe payment develops obstacle towards successful adoption of e-commerce and m-commerce. Trust plays a main role in reducing these fears. It assists in reducing these issues namely ambiguities, frauds, risks and uncertainties regarding financial transactions in online or electronic commerce and thus enhance the likelihood of maximizing customers to adopt mobile banking [63-66].

2.3 Identity theft:

Ghosh and Swaminatha [67] elucidated that users of m-commerce have to tolerate probable higher risk related to security because of telecommunication technology nature. Mobile transmission and data roam through air so such data can be easily captured. This makes applications of m-commerce more vulnerable to breaches of data which result in identity theft. Various scholars have found that identity theft is one of serious privacy concerns faced by the users of m-commerce activities and applications [68] [69] [70] [71] [72] [73]. More than 13 million of users have become the victim in the perceived risk of identity theft in 2013 as illustrated from Javelin report [74]

It was described by OECD that when 3rd party adopts financial information of customer to buy something in online without knowledge or consent of the customer then an unauthorized charge happens. Stakeholders pointed out that such kind of fraud remains main concern in the mobile and online payments. In most of the cases, such fraud is done when a fake user obtains and adopts the personal information that a consumer has given in earlier online session and that is known as inline identity theft [75] [76].

It was proven by SAP [77] and Chen and Dai [78] that customers' fear and worry about probable identity theft and breaches of data through mobile interaction can change their favourable attitude or perception towards m-commerce to unfavourable and less favourable. Centre for internet safety [79] conducted a research to examine about privacy and the internet. 85 percent of Australians online user believed that notification for data breach must be compulsory for business. 86 per cent of user stated as main issue in m-commerce activities is identity theft and 83 per cent of user found that loss of financial data as the greatest privacy issue.

According to government accountability office [80] identity theft is major threats to customers linked with tracking and profiling. It entails utilizes of somebody's personal data for committing fraudulent or other crimes. Scassa and Deturbide [81] acknowledged that profiling depends on combination of customer information which has been de-acknowledged i.e. stripped of data which allow the recognition of any individual's source. Identity theft would result in severe economic hardship for customers [82].

Singh and Aggarwal [83] found that female consumers fear more regarding privacy and security of m-commerce when compared to male consumers. Female consumers will get fear due to loss of mobile phone or identity theft. It might be be-

cause of sensitivity regarding society issues and social stigma related with female than males. Internet speed does not permit customers to carry out the payments efficiently. At the same time, identity theft, phishing and hacking are seen always, since customers do not have software for security purposes in their mobiles. When users are accessing mobile applications their personal detail, identity and credentials of bank is obtained by app store. While making a payment, details of the user is carry forwarded to 3rd party and if something goes incorrect either orders remains pending or have to do transaction again and most of the times process will be cancelled. In such cases, users' identity can be lost [84] [85].

Khasawneh [86] carried out a research to study about the consumer attitudes towards adoption of mobile banking. Social and privacy risks have developed as negative factors which influence attitude of customers towards mobile banking and as a result their overall purpose for adopting mobile banking. 1stly, the experimental proof of this investigation pointed out that security or privacy risks is the most powerful and significant factor which negatively influence the attitudes of consumers towards mobile banking which imply that customers those see mobile banking as platform which is not secure and also worry about identity theft and fraudulent activities.

2.4 Lack of transparency:

Johnston et al [87] found that institutional based risks such as transparency issue and lack of knowledge regarding rights of consumers and communications interceptions for security were found among institutions of government. As stated by Joubert and Belle [59] that transactions in the m-commerce are characterized by anonymous vendors, complex technology, convoluted communications between stakeholders and lack of transparency [88] [89]. Numerous scholars and investigators have noticed that lack of transparency [18] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99] was found to be one of the main barriers which affect to switch towards mobile commerce applications.

In the transaction system of mobile finance, characteristics of system will be less transparent to customers [100]. When focusing on the issues of transparency in applications of mobile money in region of Africa, developers have illustrated few advantages of electronic cash. It is the digital currency wherein funds cannot be spent for 2nd time and transactions are anonymous. Bitcoin is most famous demonstration of electronic cash, however regulatory and technical issues exist related to transparency as explained in Bitcoin project [101]. It was elucidated that customers also transmit payment, even though they are not able to compare amount or to identify the exact cost of transmitting amount because of the opaque of pricing in the remittance industry. There is no transparency in communication about all fees which are applicable encompassing the conversion of currency rate applicable to customer [102-104]. Research carried out by UK national consumers council [105] and Ofcom [106] identified that non-transparent pricing and confusing products make it time consuming or complicated when compared with deals relative to internet and mobile telephony.

With the limited protections for privacy and vulnerable cyber circumstances, needs of FAFT (financial action task force) ask numerous issues related to mobile money with specific reference to Africa. Recommendations of FATF as a service of finance are applicable to mobile money as like conventional services for banking. Worldwide attempt to fight terrorism and money laundering is appropriate to services of mobile money just as conventional banking. Reporting, verification and identification needs in the recommendations of FATF are positive effort for ensuring the applications of mobile money cannot transform as tool for laundering at mobile services. Needs for transparency of user would develop potential issues. 10th recommendation in FATF suggested that financial institutions has to perform due diligence for customer which encompasses verifying the clients identity and examining user transactions [107]. In addition to these, 11th recommendation in FATF stated that financial institutions has to maintain all transactions records for 5 years in order to allow them to fulfil quicker response with the requests of data from capable authorities. Such needs for transparency and keeping the record pose a numerous privacy issues for user in the applications of mobile money [108] [109].

It is suggested by consumer Affairs Victoria [110] that m-commerce have more particular responses related to regulation to support the development of m-commerce or resolving particular customer problems which is associated with m-commerce introduction. Such direct involvement concentrates on enhancing the m-commerce transactions transparency for customers and address privacy concerns with valuable invasiveness of mobile technology or applications when adopted for commercial intentions.

3. DISCUSSION

Table 2: Privacy issues associated with mobile commerce based applications

Misuse of data	Lack of trust	Identity theft	Lack of transparency
Misuse of data would develop severe privacy concerns	Lack of trust is one of main obstacle among privacy issues faced by users in adopting the mobile commerce technology	Identity theft is one of serious privacy concerns faced by the users of m-commerce activities and applications	Lack of transparency was found to be one of the main barriers in mobile commerce applications
Customers face 2 types of privacy risks namely illegal access to personal information, threat of secondary use of data	Fake usage occurs due to illegal transaction that minimizes the trust level among customers of mobile banking	Applications of m-commerce more vulnerable to breaches of data which result in identity theft	Transactions in the m-commerce are characterized by anonymous vendors, complex and lack of transparency
Loss of control over data i.e. misuse of data is vital to the idea of privacy invasion	Trust is important in some cases which are found to be risky, and mobile commerce shows users to new risks and vulnerabilities.	Customers' fear and worry about probable identity theft and breaches of data through mobile interaction would change their attitude	Non-transparent pricing and confusing products make it time consuming or complicated
Privacy of information is very significant for protecting customers from turning into victim towards changing information, unauthorized access and misuse of data by other parties	Lack of trust and fear of privacy issues encompassing fear of losing personal data, develops obstacle towards successful adoption of m-commerce	Identity theft is major threats to customers linked with tracking and profiling	There is no transparency in communication about all fees which are applicable encompassing the conversion of currency rate applicable to customer
RFID, barcodes and positioning adopted for enhancing privacy	Level of trust among customer decreases due to loss of money in the m-commerce activities	Female consumers fear about privacy issues of m-commerce than male	Privacy risks and customers transparency can be enhanced through direct involvement

Table 2 depicts privacy issues associated with mobile commerce based applications.

From the above literature, it was evident that most of the consumers are worried about giving their personal information to the service provider, vendors due to lack of trust, misuse of data, identity theft and lack of transparency.

Data given by the customer for a specific purpose needs to be clearly mentioned in the identification (ID) given. Purpose for carrying out the transaction and date has to be specified during transactions. Thus ID given by the customer that day cannot be reproduced for any other purpose in the future. If this is followed then misuse of data can be rectified to certain extent. ID Terms and conditions mentioned in the applications of mobile commerce has to be clearly explained and it should be in understandable manner. All information like direct costs, indirect cost and other details has to be mentioned clearly for avoiding transparency issue among customers. Security number given by the provider should not be shared with unknown person during transactions. Cross check and double check has to be done when providing information to vendors, merchants and more. User has to be careful in choosing their vendor, merchants to execute their mobile transactions. In such way, identity theft can be prevented to certain extent. Trust plays a vital role in adopting mobile commerce applications among users. Acquiring trust among users is not easy task. Therefore service providers have to focus more on trust factor. Service providers have to keep up the promises they have given, illegal and valid information has to be given and so on in order to maintain and build trust among users. It is clear that rectifying identity theft, misuse of data and lack of transparency can enhance the trust level among customers towards adopting mobile commerce. All privacy issues (misuse of data, lack of transparency, lack of trust and identity theft) associated with m-commerce based applications cannot be given permanent resolution but can be prevented and avoided to certain extent.

4 CONCLUSION AND FUTURE WORK:

Mobile commerce has acquired more attention all over the globe. Nowadays many consumers have desire and started to use mobile commerce based applications. This research have reviewed the privacy issues were taken into consideration such as lack of transparency, lack of trust, misuse of data and identity theft with specific reference to mobile commerce applications. This research utilizes only secondary data of research. Service providers of mobile commerce have to concentrate on these privacy issues in order to attract existing customers as well as to acquire new customers. They have to focus on addressing this issue with help of advanced technologies and tools. It is clear that rectifying misuse of data, identity theft and lack of transparency can enhance the trust level among customers towards adopting mobile commerce. Future work can be expanded by other investigators in a quantitative way of approach. It can be conducted quantitatively by collecting the primary data from users of mobile commerce applications belonging to a particular region through statistical tools.

ACKNOWLEDGMENT

We express our sincere gratitude to our company for their inspiring guidance and support throughout the course of this project. We thank our company employees for giving moral support and abundant blessing in all the activities

REFERENCES

[1] Felicitta.J and Jayanthi.J.G (2009), The impact of m-commerce in global perspective-A SWOT analysis, Conf on electronics, hardware, wireless and communications

[2] Anckar.B and D'Incau (2002), Value added services in mobile commerce: An Analytical framework and empirical findings from a nationals consumer survey, Proceedings of the 35th Hawaii International conference on systems science

[3] Mobiloity.I (2001), Fundamentals of m-business, an M-business.

[4] Buse.S (2002), Der mobile Erfolg-Empirischen uter-suchung in ausgewahlten Branchten in Keuper, F.(eds): e-business and mobile business, pp 91-117.

[5] Muller-Veerse.F (2000), Mobile commerce report, world wide web, retrieved on: 23rd march 2016, Retrieved from: http://www.dad.be/library/pdf/durlacher1.pdf

[6] Laukkanen.T (2007), Internet vs mobile banking: Comparing customer value perceptions, Business process management journal, vol 13, no 6, pp: 788-797

[7] Laforet.S and Li.X (2005), Consumers' attitudes towards online and mobile banking in China, The international journal of bank marketing, vol 23, no 5, pp: 362-380

[8] Qingfei.M, Ji.S and Qu.G (2008), Mobile commerce user acceptance study in China: a revised UTAUT model, Tsinghua science and technology, vol 13, no 3, pp: 246-257.

[9] Lee.M.S, McGoldrick.J.P, Keeling.A.K and Doherty.J (2003), Using ZMET to explore barriers to the adoption of 3G mobile banking services, international journal of retail and distribution management, vol 31, no 6, pp: 340-348

[10] Varshney as cited in Jain.S (2015), A review of SWOT Analysis of M-commerce in India, International journal of management and commerce innovation, vol 3, iss 1, pp: 712-716.

[11] Recklies.O (2001), M-commerce, the next hype?, OC, march.

[12] MRI and Rakuten, Inc. (2004), Tenth Survey of Users for Mobile Contents / Services, July (in Japanese).

[13] Gururajan.R (2006), A Discussion on Security Risks in Mobile commerce, e-business review, 7(2), pp; 9-39.

[14] Sharma.P, and Singh.P (2009). Users 'perception about mobile banking- with special reference to Indore & around. Review of Business & Technology Research, 2(1), 1-4

[15] Kazi.A and Mannan.M (2013), Factors affecting adoption of mobile banking in Pakistan: Empirical Evidence, International Journal of research in business and social science, vol 2, no 3, pp: 54-61

[16] McGuire.M and Dowling.S (2013). Cyber-enabled crimes-fraud and theft, Retrieved on: 21st March 2016, Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

[17] Matt.P (2013), Mobile app madness: Two Dos and Two Don'ts for retailers, Retrieved on: 20th march 2016, Retrieved from: http://www.retailsolutionsonline.com/doc/mobile-app-madness-two-dos-and-two-donts-for-retailers-0001

[18] Culnan.J and Armstrong.K (1999), Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science, 10 (1) : 104-115.

[19] Zweig.D and Webster.J (2002) "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," Journal of Organizational Behavior (23), pp. 605-633

[20] Zweig.D, and Webster. J (2003), Personality as a Moderator of Monitoring Acceptance, Computers in Human Behavior (19), pp. 479-493

[21] Narasimhan.A.L and Geetha.A (2002), The Future of M–commerce. Electronics for You. May 2002.

[22] CAV, M-Commerce: What is it? What Will it Mean for Consumers?, Victorian Government Department of Justice, Victoria, Australia, June 2002, Retrieved on: 21st march 2016, Retrieved from: http://www.consumer.vic.gov.au/CA256902000FE154/Lookup/CAV_Publications_Reports_and_Guidelines/$file/mcommerce.pdf

[23] Jackson.M, A Data protection Framework for Technology Department, Telecommunication Journal of Australia, vol. 54, no. 2, pp. 43-51, 2004

[24] Singh.S and Cassar-Bartolo.K, The privacy of money and health: A User Study, in Proceedings of OzCHI 2004, Wollongong, Australia, 2004

[25] Tan.M., and Teo.T. S. H. (2000). Factors influencing the adoption of internet banking. Journal of the Association for Information Systems, 1(5), 1-44

[26] Gu.J. C, Lee.S.C, and Suh.Y. H (2009). Determinants of behavioral intention to mobile banking. Expert Systems with Applications, 36, 11605-11616.

[27] Luo.X, Li. H, Zhang.J and Shim.J.P (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decision Support Systems, 49(2), 222-234.

[28] Al-Jabri.I.M, and Sohail.M. S. (2012). Mobile banking adoption: Application of Diffusion of Innovation Theory. Journal of Electronic Commerce Research, 13(4), 379-391.

[29] Prakash.K and Balachandra (2014), Mobile computing and M-commerce security issues, computer science and information technology, pp: 205-216.

[30] Satariano.A, and MacMillan.D (2012). Anarchy in the App Store. Bloomberg BusinessWeek

[31] Niranjanamurthy.M, Kavyashree.N, Jagannath.S and Chahar.D (2013), Analysis of e-commerce and m-commerce advantages, limitations and security issues, International journal of advanced research in computer and communication engineering, vol 2, iss 6, pp: 2360-2370.

[32] Abdul.G.N, and Mohamed.S.Z (2008), Controlling Your Personal Information Disclosure,7th WSEAS International Conference on Information Security and Privacy (ISP '08) Proceedings, pp. 23-27

[33] Gao.J and Kupper.A (2006), Emerging technologies for mobile commerce, Journal of theoretical and applied electronic commerce research, vol 1.

[34] Lee.M.K.O and Turban.E 2001."A Trust model for consumer internet shopping". International Journal of Electronic Commerce, vol.6, no.1, pp. 75-91., 2001.

[35] Siau.K Sheng.H and Nah.F (2003), "Development of a framework for trust in mobile commerce", Paper presented at the Proceedings of the Second Annual Workshop on HCI Research in MIS, Seattle, WA

[36] Corbitt.B.J Thanasankit.T andYi.H (2003), "Trust and e-commerce: a study of consumer perceptions". Electronic Commerce Research and Applications, vol.2, no. 3, pp. 203-215.

[37] Carlsson.C and Carlsson.J (2005), Mobile Commerce: Insights from Expert Surveys in Austria and Finland, 18th Bled eConference eIntegration in Action.

[38] Lu.J, Yu.C.S and Liu.C (2005), "Facilitating conditions, wireless trust and adoption intention".Journal of Computer Information Systems, vol. 46, no. 1, pp. 17-24.

[39] Wuand.J.H and Wang.S.C (2005), "What drives mobile commerce?". Information Management, vol. 42, no. 5, pp. 719-729.

[40] Park.J, and Sujin.Y (2006),"The moderating role of consumer trust and experience: value driven usage of mobile technology". International Journal of Mobile Marketing, vol. 1, no. 2, pp. 24-32.

[41] Mallat.N (2007), "Exploring consumer adoption of mobile payments – A qualitative study". The Journal of Strategic Information Systems, vol. 16, no. 4, pp. 413-432.

[42] Yeh.Y,S and Li.Y.M (2009). "Building trust in m-commerce: contributions from quality and satisfaction". Online Information Review, vol. 33, no. 6, pp. 1066-1086.

[43] Kim.C, Mirusmonov.M and Lee.I (2010), "An empirical examination of factors influencing the intention to use mobile payment". Computer Human Behaviour, vol. 26, no.3,pp. 310-322

[44] Joubert.J and Belle.J (2013), The role of trust and risk in mobile commerce adoption within South Africa, International Journal of business, humanities and technology, vol 3, no 2, pp: 27-38

[45] Payal and Juneja.N (2013), Application of M-commerce in India, International journal of advanced research in IT and engineering, vol 2, no 4, pp:62-67.

[46] Saleh.I and Mashhour.A (2014), Consumer attitude towards M-commerce: The perceived level of security and role of trust, Journal of emerging trends in computing and information sciences,

[47] Siau.K and Shen.Z (2003), "Building customer trust in mobile commerce," Communications of the ACM, vol. 46, pp. 91-94.

[48] Qingfei.M, Decai.M and Qiuyan.Z (2008),"An empirical study on trust in mobile commerce adoption". Paper presented at the Service Operations and Logistics, and Informatics, IEEE/SOLI 2008. IEEE International Conference

[49] Chou.Y, Lee.C, and Chung.J (2004), —Understanding m-commerce payment systems through the analytic hierarchy process,‖ Journal of Business Research, vol. 57, Dec., pp. 1423-1430.

[50] Flavian.C, and Guinaliu.M (2006), Consumer trust, perceived security, and privacy policy: three basic elements of loyalty to a web site, Industrial Management & Data Systems, Vol. 106 No. 5/6, pp. 601-20.

[51] Harris.A (2002), Privacy on and off the internet: what consumers want, Retrieved on: 21st march 2016, Retrieved from: www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf.

[52] Kruck.S.E, Gottovi.D, Moghadami.F, Broom.R and Forcht.K.A (2002), Protecting personal privacy on the internet, Information Management & Computer Security, Vol. 10 No. 2, pp. 77-84.

[53] Brown.M and Muchira.R (2004), Investigating the relationship between internet privacy concerns and online purchase behaviour, Journal of electronic commerce research, vol 5, no 1, pp: 63-70.

[54] Dahlberg.T, Mallat.N and Oorni.A (2003), Trust Enhanced Technology Acceptance Model: Consumer acceptance of mobile payment solutions. Proceedings of the Stockholm Mobility Roundtable

[55] Schmidt-Belz. B (2003), Aspects of user trust in mobile guides. Workshop HCI in mobile guides

[56] De Ruyter.K, Kleijnen.M and Wetzels.M (2002), Factors influencing the adoption of mobile gaming services. Mobile Commerce: Technology, Theory and Applications, Eds: Mennecke, Strader, Idea Group Publishing, Hershey, PA: 202-217

[57] Zarmpou.T, Saprikis.V, Vlachopoulou.M and Singh.G (2010), "Investigating the Influential Factors towards Mobile Services Adoption in Greece.

[58] Min.Q, Ji.S and Qu.G (2008), "Mobile commerce user acceptance study in China: a revised UTAUT model," Tsinghua Science & Technology, vol.13, pp. 257-264.

[59] Joubert.J and Van Belle.J.P, "The importance of trust and risk in M-commerce: A South African perspective," 2009, pp. 10-12.

[60] Tarasewich.P (2003) Designing Mobile Commerce Applications. Communications of the ACM, 46, 57-60

[61] Hillman.S, Neustaedter.C, Bowes.J and Antle.A (2012), Soft Trust and m-commerce shopping behaviours, ACM.

[62] Rehman.S and Coughlan.J (2011), Building trust of mobile users and their adoption of m-commerce, World Academy of science, engineering and technology.

[63] Suh.M, and Han.I (2002). Effect of trust on customer acceptance of internet banking. Electronic Commerce Research and Application, 1(3), 247–263

[64] Wang.W and Benbasat.I (2005). Trust in and adoption of online recommendation agents. Journal of the Association for Information Systems, 6(3), 72–101.

[65] Luarn.P and Lin. H (2005), "Toward an understanding of the behavioural intention to use Mobile banking", Computers in Human Behaviour, Vol. 21, pp. 873-91.

[66] Pavlov, 2003 as cited in Mazhar.F (2014), An Investigation of factors affecting usage and adoption of internet and mobile banking in Pakistan, International journal of accounting and financial reporting, vol 4, no 2, pp: 478-501.

[67] Ghosh.A.K and Swaminatha.T.M (2001), Software security and privacy risk in mobile e-commerce, Communications of the ACM, vol 44, iss 2, pp: 51-57

[68] Schoder.D and Yin.P.L (2000), "Building Firm Trust Online", Communications of ACM, vol. 43, no. 12, pp. 73-79.

[69] Philippa.L and John.L (2003), Identity Theft: The Need for Better Consumer Protection, Public Interest Advocacy Centre, PIAC.

[70] Grami.A and Schell.B.H (2004). Future Trends in Mobile Commerce: Service offerings, technological advances and security challenges. Proceedings of the 2nd Annual Conference on Privacy, Security and Trust.

[71] Hildebrandt.M (2008). Profiling and the rule of law. Identity in the Information Society, 1, 55-70

[72] Mantell.R (2008)., 'Identity theft is top consumer complaint,' Market Watch

[73] Urban.J.M and Hoofnagle. C.J and Li.S (2012). Mobile Phones and Privacy. BCLT Research Paper.

[74] Javelin Report (2014), 2014 Identity fraud report: Card data breaches and inadequate consumer password habits fuel distributing fraud trends, retrieved on: 21st march 2016, Retrieved from: https://www.javelinstrategy.com/brochure/314

[75] OECD (2008a), Policy Guidance on Online Identity Theft, OECD, Paris, 2008, Retrieved on: 21st march 2016, Retrieved from: www.oecd.org/dataoecd/49/39/40879136.pdf.

[76] OECD (2008b), Scoping Paper on Online Identity Theft, Retrieved on: 21st march 2016, Retrieved from: www.oecd.org/dataoecd/35/24/40644196.pdf.

[77] SAP, "The mobile consumer insights on global trends impacting mobile momentum and customer engagement," retrieved on: 21st march 2016, Retrieved from:http://www.sap.com/pc/tech/mobile/featured/offers/mobile-consumer-behaivor-report.html, 2013

[78] Chen.Y and Dai.H (2014), Do innovators concern less about security and value new technologies more? A case of mobile commerce, Journal of information technology management, no 4, pp: 13-26

[79] Centre for internet safety (2012), Privacy and the internet, CIS.

[80] Government Accountability Office. (2012). Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO.

[81] Scassa.T and Deturbide.M (2012). Electronic Commerce and Internet Law in Canada (2nd ed.). Toronto: CCH Canadian Limited.

[82] Sproule.S and Archer.N (2008). Measuring Identity Theft in Canada: 2008 Consumer Survey—Working Paper #23. McMaster University

[83] Singh.K and Aggarwal.H (2013), Critical factors in consumers perceptions towards mobile commerce in E-governance implementation: An Indian perspective, International journal of engineering and advanced technology, vol 2, iss 3, pp: 513-520.

[84] Agarwal.A and Bhatawal.H (2015), M commerce in India: Promise and problems, International journal of research in computer and communication technology, vol 4, iss 4, 273-276

[85] Gupta.C, Chandhok.A and Gupta.M (2016), Hardship of M-commerce in India: Problems, Issues and Challenges, Journal of business and management, vol 18, iss 1, pp: 22-26.

[86] Khasawneh.M.H.A(2015), A mobile banking adoption model in the Jordanian Market: An Integration of TAM with perceived risks and perceived benefits, Journal of internet banking and commerce, vol 20, iss 3, pp:1-13.
[87] Johnston.A.C, Warkentin.M (2002). The online consumer trust construct: A web merchant practitioner perspective. Proceedings of the Seventh Annual Conference, Southern Association for Information Systems: 221-226
[88] Federal Trade Commission. (February 2013). Mobile privacy disclosures: Building trust through transparency. FTC Staff Report.
[89] NTIA. (2013). NTIA privacy multi-stakeholder process: Mobile applications transparency. Retrieved on: 22nd march 2016, Retrieved from: www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency
[90] Hoffman.D.L, Novak.T.P and Peralta.M (1999) 'Building Consumer Trust Online', Communications of the ACM 42(4): 80–5.
[91] Langheinrich.M (2002) 'Privacy Invasions in Ubiquitous Computing', Privacy in Ubicomp'2002, Go¨teborg, Sweden
[92] Hann.I.H, Kui.K. L, Lee.T.S and Png.I.P.L (2002) 'Online Information Privacy: Measuring the Cost–Benefit Trade-Off', Proceedings of the 23rd International Conference on Information Systems
[93] Elliott.T and Cunningham.D (2005) 'The Burden of Trusted Information', DM Review, 18–33.
[94] EC (European Commission) (2006), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communication networks and services {COM(2006)334 final}—Proposed Changes, Staff Working Document, Brussels, 28 June, SEC(2006) 816
[95] Galanxhi.H and Nah.F (2006), Privacy issues in the Era of ubiquitous commerce, Electornic markets.
[96] Andrew.W (2009), Mobile banking in developing countries (a case study on Kenya), UAPS.
[97] Maimbo.S, Tania.S, and Nicholas.S (2011), "Facilitating Cross-Border Mobile Banking in Southern Africa." Africa Trade Policy Note 1, World Bank, Washington, DC
[98] Joppien.J, Niermeijer.G and Niks.M.C (2013, March). Exploring New Possibilities For User-Centred E-Ticketing (research report) Delft University of Technology, Delft, the Netherlands
[99] Niks.M.C (2013), Making the invisible visible, TUDelft.
[100] Chogi.B.F.M (2006), The Impact of Mobile Communication Technologies in Medium and Small Enterprises: Case Study of Nairobi City, MSc. Thesis submitted at the University of Nairobi, School of computing and Informatics.
[101] Bitcoin project (n,d), Mobile payments, retrieved on: 22nd march 2016, Retrieved from: http://bitcoin.org/
[102] Sanket,M, Dilip.R and Silwal.A (2011), Outlook for Remittance Flows 2011-13, Migration and development brief 16,Migration and development Unit, World Bank) 2011.
[103] CI (2012), CI The remittances game of chance: playing with loaded dice, 2012
[104] African development bank (2012), Financial inclusion and integration through mobile payments and transfer. African Development Bank & Yes Bank. 2012
[105] UK national consumers council (2006) as cited in OECD (2008c), Enhancing competition in telecommunications: protecting and empowering consumers, Ministerial background report.
[106] Ofcom (2006), —Consumer Experience Research‖, Annex 4, —Consumer Decision-Making in the Telecoms Market, Report on research findings, Research Annex, November 16
[107] Economist (2012), Mobile Money in Africa: Press 1 for Modernity, THE ECONOMIST
[108] FIN. Action task force, international standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations (2012), Retrieved on: 22nd March 2016, Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf.
[109] Harris.A, Goodman.S and Traynor.P (2013), Privacy and security concerns associated with mobile money applications in Africa, Washington journal of law, technology and arts, vol 8, iss 3, mobile money symposium.
[110] Consumer affairs Victoria (2004), Considering the implications of m-commerce-A consumer perspective, issue paper, standing committee of officials of consumer affairs.