Modern Applied Science; Vol. 13, No. 12; 2019
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Consumers Trust, Privacy and Security Issues on Mobile Commerce Websites

Mohammad awni ahmad mahmoud[1], laith Talal khrais[2], Rasha mohammad alolayan[1], Asyah muzahim alkaabi[1], Sara qasem Al- suwaidi[3], Bushra Abdulmohsin Alghamdi[3] & Hadeel Fouad Aljuwaie[3]

[1] Mis department, Applied studies and community services, Imam Abdulrahman bin Faisal University,Dammam, Saudi Arabia

[2] Business management department, Applied studies and community services, Imam Abdulrahman bin Faisal University, Dammam, Saudi Arabia

[3] Accounting department, Applied studies and community services, Imam Abdulrahman bin Faisal University, Dammam, Saudi Arabia

Correspondence: Mohammad awni ahmad mahmoud, Mis department, Applied studies and community services, Imam Abdulrahman bin Faisal University, Dammam, Saudi Arabia. E-mail: maamahmoud@iau.edu.sa

Received: September 22, 2019 Accepted: November 11, 2019 Online Published: November 13, 2019

doi:10.5539/mas.v13n12p21 URL: https://doi.org/10.5539/mas.v13n12p21

Abstract

The proliferation of mobile devices and the increased adoption of the internet across the globe has led to the rise of m-commerce. reports highlight that in spite of the different advancements in the technology, trust in the platform is still a significant hindrance to its adoption. Consequently, the current study seeks to identify privacy and security issues affecting m-commerce users of three shopping sites: Amazon, Alibaba and eBay. The aim here is to develop recommendations that mitigate these challenges. The expected output of the study is an anticipation for insights regarding user perspectives on trust in m-commerce and as a result, contribute to existent knowledge in the area benefitting regulatory bodies and online vendors

Keywords: e-commerce, m-commerce, privacy, security, low adoption, wireless communication

1. Introduction

The advancement of technology and the wide-scale adoption of the internet has led to an upsurge in the ubiquity of mobile devices and as a result, the increased adoption of mobile computing (Noor et al., 2018). Consequently, activities previously completed only through traditional desktop computers are now being easily undertaken via mobile devices. Rajhashyamala et al. (2017) note that mobile computing is leading change in the manner in which businesses communicate and carry out their daily operations as a result of their efficiency, productivity and connectivity.

Despite mobile computing offering advantages such as mobility and access to diverse network types, it is however limited due to aspects such as intermittent network disconnection, poor reliability and security. Similarly, Ibukun and Daramola (2015) add that mobile computing is hampered by existent constraints in mobile devices in terms of their hardware, software and connectivity. Subsequently, users undertaking their computing activities in mobile environments encounter challenges such as limited computational power, reduced storage sizes and limited battery life.

A key solution to overcoming such challenges is the adoption of Mobile Cloud Computing (MCC) (Ibukun & Daramola, 2015). With the Mobile Cloud Computing (MCC) paradigm, the benefits of mobile computing are combined with those of cloud computing thereby enabling devices with limited capabilities and resources to undertake powerful computations that run on the cloud. Due to such capabilities, mobile cloud computing has been adopted across diverse sectors ranging from health and education to e-commerce and entertainment (Ibukun & Daramola, 2015).

A third challenge pertains to the aspect of energy efficiency where compute-intensive aspects in mobile environments such as hardware and software resources drain a significant amount of energy (GU Et Al., 2018). As such, a need arises to offload some of these aspects to the cloud in order to save both time and energy. Fourth,

is the aspect of heterogeneity where a challenge arises in supporting diverse devices accessing the cloud environment through diverse network types (Noor et al., 2018).

Finally, there is a concern for privacy and security of the paradigm (Mollah, Azad & Vasilakos, 2017). The researchers argue that as mobile users employ heterogeneous channels of communication to transfer data to and from the cloud data centers, diverse vulnerabilities are introduced in the given channels. As such, attackers might exploit such vulnerabilities thereby compromising the given data.

Further, since mobile computing utilizes aspects such as location-based data (e.g. GPS), malicious users are likely to eavesdrop on the networks thereby interfering with the privacy concerns. A study by Kim and Kim (2016) identified trust and convenience as the two key factors influencing user decisions on the adoption of mobile cloud computing. Subsequently, this indicates the importance of ensuring optimum security and privacy of the paradigm in order to gain user support.

One of the sectors where cloud data security and privacy is of high concern is mobile commerce (m-commerce) (Sultan, Khan & Khan, 2016). The authors posit that concerns for privacy and security arise due to the inherent nature of m-commerce. On the one hand, since m-commerce is primarily undertaken in handheld devices such as P.D.A.s, tablets and mobile phones, access to user geo-location

data introduces privacy and security concerns. On the other hand, the functional limitations of mobile devices make it difficult to implement security measures already in use in the e-commerce platform,

e.g. cookies and active server pages. Further, since m-commerce is more personalized to suit user requirements, concerns for the privacy of the personal information are also high.

2. Problem Statement

Given the uniqueness of the architecture of the mobile cloud computing paradigm, a need arises to provide robust, scalable and efficient mechanisms to guarantee the security and privacy of mobile users (Noor et al., 2018). Furthermore, the uniqueness of m-commerce in terms of its enabling technology and infrastructure further intensifies the need to address privacy and security in Mobile Cloud Computing (MCC) enabled m-commerce. Consequently, this paper seeks to identify the existent issues associated with Mobile Cloud Computing (MCC) enabled m-commerce and propose various recommendations to mitigate such challenges.

3. Research Questions

1. What are some of the security and privacy issues facing mobile cloud computing users of m- commerce applications?

2. What are some of the recommendations that can be formulated to help solve the identified challenges?

4. Research Objectives

1. To identify security and privacy issues facing mobile cloud computing users of m-commerce applications.

2. To formulate various recommendations to help solve the identified challenges in mobile cloud computing m-commerce applications.

5. Scope of the Study

While m-commerce applications broadly cover three aspects: finance; purchasing and advertising, the current study limits itself to m-commerce in the purchasing category. As such, it seeks to investigate the existent privacy and security issues affecting m-commerce users who purchase goods and services from online merchants. Similarly, it proposes recommendations and mitigation approaches for only such users. In regard to online merchants, three online providers: Amazon; eBay and Alibaba are selected based on their popularity on a global scale. In addition, only m-commerce users from the researcher's country will be assessed.

6. Significance of the Study

Trust is a key factor that influences m-commerce customer loyalty (Lee & Wong, 2016). As such, identifying security and privacy issues associated with m-commerce and providing recommendations to such issues further improves their trust towards the technology thereby enhancing its adoption. In addition, the study offers important insights to online merchants in regard to privacy and security concerns of m-commerce users. Such insights are useful in improving their services to meet user needs better. Finally, the study also provides important insights into national and international organizations that regulate data privacy and security in the sector.

7. Literature Review

By definition, m-commerce is delineated as any transaction in which there occurs transfer of ownership or rights to enable the use of goods or services, and that is launched and terminated using mobile access to computer-mediated networks with the help of mobile devices (Lee & Wong, 2016). As such, it is considered to be a subset of e-commerce as commercial transactions are conducted via the internet medium. An important aspect to note, however, is that over the years, there has been an increase in the growth of m-commerce due to factors such as increased internet adoption and familiarization of consumers with mobile devices (Lee & Wong, 2016).

Chao (2017) further reports that m-commerce has risen to be one of the most important sectors in the U.S. retail business with smartphones having penetrated to nearly 80% of its population by 2017. Consequently, more transactions are being completed via mobile phones as compared to computers due to the features of m-commerce that make it more feasible than its predecessor, e-commerce. Such features include its content characteristics, service and overall devices (Hussain, Mahmood & Naser, 2017). Further, with the portability of mobile devices, users can complete transactions anywhere and at any time.

While m-commerce is considered a subset of e-commerce, it is important to note that there are significant differences between the two which introduce different security and privacy issues. First, as Desai (2016) notes, m-commerce is conducted through mobile and wireless devices using wireless technology while e-commerce is conducted through laptops and wired computers. The implication of this difference in devices used is that the former holds immense potential for higher personalization compared to the latter especially since wireless devices are embedded with geolocation services and can inform the location of customers. Nonetheless, higher levels of personalization lead to further privacy and security issues due to the increased amounts of data shared by users.

A second notable difference between the m-commerce and e-commerce lies in the fact that the two are powered by different enabling technologies (Mishra et al., 2016). Given that mobile devices rely on Wireless Application Protocol (WAP) to receive web information and access the internet, this creates a compatibility challenge with other technologies that are already in use in the e-commerce platform. As a result, security technologies that operate in the e-commerce platform such as cookies, Java and Active Server Pages are limited in m-commerce platforms thereby creating further security challenges.

Thirdly, there also exists a difference in the communication mode used by the two platforms as m-commerce primarily uses wireless networks while e-commerce relies on wired networks for desktop computers though wireless networks are also used with laptops (Desai, 2016). The use of wireless networks creates convenience in using technology as users can complete transactions independent of their location. However, it also introduces a security vulnerability as malicious users can infiltrate such networks and exploit weaknesses within them to their advantage.

Finally, there also exists a difference in the languages used in developing applications in the two platforms with Wireless Markup Language (WML) being used in m-commerce while HyperText Transfer Protocol (HTTP) is used in the e-commerce platform (Huang et al., 2016). The implication of the use of different developmental languages and communication protocols is that there arise significant limitations and compatibility issues in the former's case thereby impacting security.

While the review of the differences between m-commerce and e-commerce provides important insights on the security vulnerabilities associated with the former, it is important to note that the two are built on the cloud computing paradigm (Desai, 2016). The researcher notes that with this paradigm, applications are run on remote servers with all the processing being undertaken on the remote servers with the results being relayed to the user. As such, in both instances, the web and mobile devices, processing of the commercial transactions occur in remote servers with the results of the processing being relayed in the devices.

Understanding the underlying paradigm which powers both m-commerce and e-commerce is important since it introduces insights regarding the security and privacy of the users in both cases. However, since the current paper focuses on the former, concerns for user security and privacy are only examined in m-commerce. In the beginning, it is important to understand the definition of the two terms which are often used interchangeably and in the same context.

The definition of privacy adopted in this paper considers it as the concern that consumers of the internet have in sustaining their personal information such as data and knowledge about themselves, their activities and actions, securely in their control without such control being compromised by other entities or individuals (Lu et al., 2015).

This definition implies that it provides users with some say over how to and what to reveal about their personal information. As such, privacy concerns the control users have to their data.

On the other hand, information security, in the context of e-commerce, is in simple terms described as a mechanism that allows authorized people to transact business securely and efficiently over the internet while keeping unauthorized people away from the valuable information (Horne, Ahmad & Maynard, 2015). As such, security concerns aspects that ensure that the valuable information in e-commerce platforms is not accessed, destroyed or compromised by unauthorized users.

The definitions imply that they highlight the notion of trust by users on the technology and the different online merchants. On the one hand, privacy implies that users gain interest regarding the use of the personal data they share with online vendors while on the other hand, security implies that they as well become concerned over the measures put in place to ensure their valuable information such as credit cards details are not compromised by unauthorized users.

Gaining trust in m-commerce is especially significant since the platform enables finer personalization as handheld devices are used to conduct commercial transactions. Similarly, the limitations of handheld devices concerning processor speed, bandwidth and memory further imply that the security measures put in place in e-commerce platforms are limited in m-commerce. Also, the predominant reliance on wireless technology and different communication protocols further aggravate security and privacy concerns as they increase the threat surface that can be exploited by malicious users.

Ghayoumi (2016) identifies six important dimensions of e-commerce security that are also relevant to m-commerce since the latter is a subset of the former. First, is integrity which focuses on preventing unauthorized data modification while second, is non-repudiation, which emphasizes preventing one party from reneging on an agreement after the fact. Third, is authentication, which considers the authenticity of the data while fourth, is confidentiality, which protects against the unauthorized disclosure of data (Ghayoumi, 2016). Fifth is privacy which seeks to control the disclosure of data while sixth, is availability which focuses on preventing removal of data and inappropriate delays.

In regard to privacy, Ghayoumi (2016) identifies seven important types of privacy. First, is the person's privacy which focuses on keeping their bodily functions and characteristics private while second is the privacy of behavior and actions whereby user behavior and information on sensitive issues ought to be maintained in a secure manner (Ghayoumi, 2016). Third is the privacy of communication whereby concern is to ensure all types of user communication ranging from e-mail to telephone and wireless communication is not intercepted.

Fourth, is the privacy of data and images which is concerned with ensuring user data is not automatically available to third parties. Fifth, the privacy of thoughts and feelings where users should be allowed the freedom and right to think as they please without such feelings being revealed (Ghayoumi, 2016). Sixth is the privacy of location and space whereby individuals ought to have a right to move around without being tracked or monitored. Finally, the privacy of association where users have a right to associate with whomever they wish without being tracked.

While the different privacy aspects are general, in the m-commerce platform, it is important to ensure that the privacy of user communication, data, location and actions in the platform are strictly ensured. Likewise, it is important to ensure that their information is secure from unauthorized access..

A different study by Dong et al. (2017) revealed that factors such as perceived trust in service providers, perceived trust in the internet, perceived privacy, and influence of society and ease of use had an influence on the adoption of m-commerce among Chinese foreigners. As such, their study concluded that their trust on the internet was still low and that towards privacy high.

Nonetheless, there has been significant progress in tackling the privacy and security issue in m- commerce with different recommendations being cited by diverse researchers.

Nilashi et al. (2015) revealed that security, design and content factors had an impact on customer trust towards m-commerce while Plateaux et al. (2018) undertook a comparative study on the card-not- present architectures with card schemes where they highlighted the use of protocols such as 3D secure to ensure the security of m-commerce applications.

Alam (2017), on the other hand, proposed the McEliese cryptosystem to encrypt and decrypt data in m-commerce environments intending to improve its security and privacy. A different study by Heinze, Thomann and Fischer (2017) examined the resistance towards m-commerce in service-based industries such as insurance. The study revealed that a barrier to adoption exists regarding the sufficiency of the service and components of

the system.

While diverse studies highlight the importance of ensuring privacy and security of users in the m-commerce platform, the low levels of trust highlighted by reports such as IAB (2016) however, reveal a need to continually develop new insights to tackle such challenges especially in online shopping sites that have a global presence. As such, the current study seeks to fill this gap by identifying privacy and security issues still present among users and propose recommendations to mitigate them.

8. Research Limitations

Several limitations are anticipated in the study. First, since the study seeks to identify user perceptions towards security and privacy of m-commerce, a challenge is anticipated in obtaining respondents who can provide valid responses to the topic of study.

Thirdly, the data collection tools used such as questionnaires may inhibit the collection of data especially where respondents are foreigners who do not speak the English language. However, in order to mitigate this, the researcher ensures that the wording of questionnaires is simple and unambiguous. Finally, while respondents may be available to take part in the study, an additional risk anticipated is obtaining unreliable data with parts either missing or filled wrongly. The researcher intends to mitigate this challenge by providing clear instructions to guide the data collection process.

9. Research Methodology

Given that the study seeks to identify security and privacy issues facing m-commerce mobile users, the study adopts a positivist philosophy since credible data will be obtained by examining observable phenomena (Kivunja & Kuyini, 2017). A deductive research approach is further used as the researcher seeks to test hypotheses through empirical observations. Advantages of enable data to be collected from a large sample within a relatively short period and they are an inexpensive data collection method (Ponto, 2015).

A mono research method is used where data is collected using only quantitative techniques using questionnaires since they provide an efficient way to collect data from a population. The study population targeted comprises of m-commerce application users who shop from either Amazon, Alibaba or eBay. The selection of these three companies is based on the fact that they are well known internationally and as such, are at the forefront of implementing best practices in ensuring user security and privacy concerns. As such, users utilizing m-commerce applications from other companies are not used in this study.

Random sample sampling will be used to obtain 100 respondents to facilitate generalizability of the results. With the random sampling approach, samples will be drawn equitably from the study population thereby enabling generalizability. Once the data is collected, analysis will be conducted using Structured Equation Modelling (SEM) whereby logistic regression and correlation techniques will be used to obtain insights from the data. Likewise, descriptive statistics such as means, standard deviation and frequencies will be used to analyze the data. Concerns for validity and reliability are adhered to by ensuring questionnaires are worded in a simple clear language and that they are administered only on the study population. Figure 1 below summarizes the research methodology adopted.

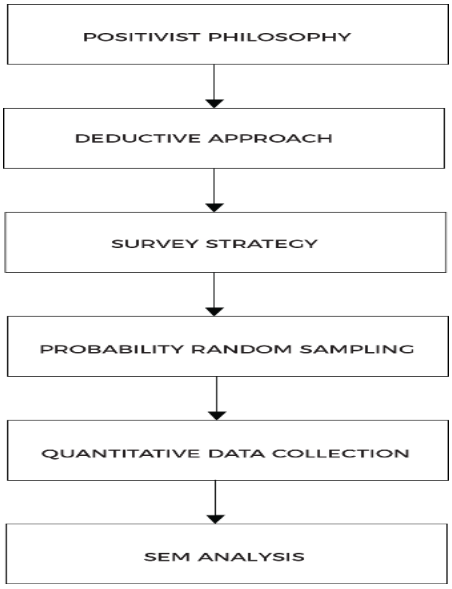

Figure 1. Research methodology (Source: author)

Figure 1 above illustrates the research methodology adopted which adheres to the research onion framework. At the onset, a positivist philosophy is utilized while as the methodology concludes, structural equation modelling is outlined as the data analysis technique.

Several ethical concerns are also considered in the study. First, appropriate permissions will be sought from the respondents before they are allowed to take part in the study. As such, questionnaires will only be administered to respondents who have consented to the participation contract. Secondly, the information gathered from the respondents will be maintained privately and confidentially to guarantee secrecy. Subsequently, the data will not be shared with third parties or sold to other institutions. Thirdly, the identity of the respondents will be hidden by assigning them pseudo names and unique identifiers in a bid to protect the identity of the respondents.

10. Research Framework

The review of diverse literature sources in the previous section revealed that m-commerce is significantly different from e-commerce concerning internet devices used, communication protocols and enabling technologies. Similarly, the limited capacity of the devices regarding processor speed and memory capacity led to the conclusion that solutions already in use in e-commerce are limited in m- commerce environments. Further study showed that trust as a social construct was heavily dependent on privacy and security. As such, trust was associated with three aspects: vendors, the m-commerce platform and the underlying internet medium.

Consequently, the research framework for this study considers privacy and security issues to arise from these three aspects. The framework is shown in figure 2 below.

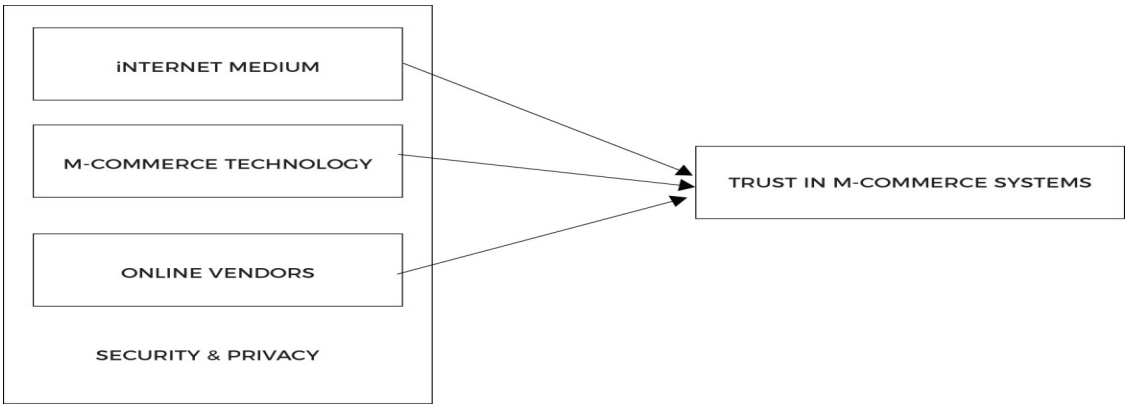

Figure 2. Research framework (Source: author)

The research framework as such hypothesizes that trust in m-commerce systems is a function of the user's perspective of security and privacy towards online vendors, m-commerce technology and the internet medium.

As such, the users' perceptions towards the three areas will be examined to identify areas that require higher attention levels. The logic behind the framework lies in the fact that user security and privacy is determined by the three aspects: online vendors; m-commerce technology and the internet medium.

As such, the study seeks to identify how user perception of trust in each of the three aspects directly influences the adoption of m-commerce applications. Consequently, this implies that different trust levels are likely to arise between the different aspects. However, the study seeks to determine the magnitude of trust in each aspect to develop appropriate recommendations. For instance, where results would indicate that lower trust exists with the m-commerce technology rather than the vendors, this would dictate that more recommendations are developed towards improving the security and privacy of the technology.

Consequently, the following hypotheses are formulated to evaluate each aspect:

H1: There is a relationship between security and privacy in the internet medium and trust in m- commerce systems,(positive).

H2: There is a relationship between security and privacy in the m-commerce technology and trust in m-commerce systems,(positive).

H3: There is a relationship between security and privacy in online vendors and trust in m-commerce systems,(positive).

Subsequently, empirical observations collected will help test the different hypotheses and identify user perceptions towards security and privacy and as a result, identify appropriate recommendations to mitigate such challenges. Logistic regression will also be used to determine the strength of the relationship based on the three different factors with the different coefficients, obtained in each case, providing an overview of the magnitude of the trust.

11. Conclusion and Expected Output

The ubiquitous nature of mobile devices coupled with the increased adoption of the internet has led to the increase in popularity of m-commerce. M-commerce essentially refers to the completion of commercial transactions via handheld devices such as smartphones and tablets. As a subset of e- commerce, m-commerce facilitates the completion of transactions in sectors such as purchasing, advertising and finance. However, differences exist between the two with a key difference being the portability and mobility of the latter.

Mobile devices are also observed to have reduced processing capacities, and they run on different communication protocols. The implications of such differences are that security solution already existent in e-commerce platforms are limited within m-commerce platforms on the one hand, while on the other, the use of different communication protocols such as WAP introduces incompatibility with available security solutions. Further, since they are embedded with geolocation hardware, they offer higher potential for personalization, often enabling user location to be used in generating recommendations in online shopping websites.

As such, the concern for privacy and security in m-commerce environments is significantly different from e-commerce given the unique characteristics of such environments. Privacy is specifically concerned with protecting the use of personal data shared with online vendors while security focuses on measures to ensure the protection of valuable user information from unauthorized users. Review of several reports indicates that the level of trust in m-commerce systems is still low especially on these two paradigms.

Further review revealed that privacy concerns with m-commerce technology include aspects such as their communication, data and actions in the platform while security features highlighted included integrity, non-repudiation, authentication, confidentiality, privacy and availability. Such aspects, while highly emphasized in e-commerce, ought to be accorded significant attention in m- commerce to improve user confidence and trust in the technology. Further, the incorporation of features such as third-party accreditation and third party privacy guarantees are also recommended as approaches to ensure privacy and security.

While several studies propose different solutions to ensure privacy and security of users in m- commerce platforms, an important finding made is that there is still significant room for improvement in mitigating such challenges. As such, the current study is based on filling this research gap, with a specific focus on users of giant m-commerce shopping sites such as Amazon, Alibaba and eBay.

The expected output of the study is that it is expected to reveal privacy and security issues associated with the internet medium, m-commerce technology and online shopping vendors based on user perceptions. Further, the study is also expected to highlight recommendations that can be implemented across the three aspects. Such findings are valuable to vendors, regulatory organizations and users in general as they provide an opportunity to

learn new insights on security and privacy.

References

Alam, M. (2017). Secure M-commerce data using post quantum cryptography in IEEE Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation. *Engineering (ICPCSI), IEEE Xplore, Chennai, India,* pp. 649-654. https://doi.org/10.1109/ICPCSI.2017.8391793

Chao, C. (2019) Emergence impacts of mobile commerce: An exploratory study. *Journal of Management and Strategy, 8*(2), 63-70. https://doi.org/10.5430/jms.v8n2p63

Desai, N. (2016) Mobile cloud computing in business, *International Journal of Information Sciences and Techniques, 6*(1/2), 197-202. https://doi.org/10.5121/ijist.2016.6221

Dong, W., Asmi, F., Zhou, R., Keren, F., & Anwar, M. (2017) Impact of trust and perceived privacy in B2C mobile apps among foreigners: A case of People's Republic of China' in IEEE Proceedings of the IEEE 14Th International Conference on E-Business Engineering (ICEBE). *IEEE Xplore*, vol. 1,Shanghai, China, pp. 189-194. https://doi.org/10.1109/ICEBE.2017.37

Ghayoumi, M. (2016). Review of security and privacy issues in e-commerce. In *CSREA Press Proceedings of the International Conference on e-Learning, e-Bus., EIS, and e-Gov*, EEE'16, Las Vegas, Nevada, USA, pp. 156-160.

Gu, F., Niu, J., Qi, Z., & Atiquzzaman, M. (2018) Partitioning and offloading in smart mobile devices for mobile cloud computing: State of the art and future directions. *Journal of Network and Computer Applications, 119*, pp. 83-96. https://doi.org/10.1016/j.jnca.2018.06.009

Heinze, J., Thomann, M., & Fischer, P. (2017) Ladders to m-commerce resistance: A qualitative means-end approach, *Computers in Human Behavior, 73*, pp. 362-374, August. https://doi.org/10.1016/j.chb.2017.03.059

Horne, C., Ahmad, A., & Maynard, S. (2015). Information security strategy in organisations: Review, discussion and future research directions. In *ACIS Proceedings of the Australasian Conference on Information Systems*. Adelaide, Australia.

Huang, X., Bao, J., Dai, X., Singh, E., Huang, W., & Huang, C. (2016) M&E-NetPay: A micropayment system for mobile and electronic commerce. *Symmetry, 8*(8), 74. https://doi.org/10.3390/sym8080074

Hussain, A., Mahmood, A., & Naser, R. (2017) Investigating the effect of m-commerce design usability on customers' trust' in *AIP conference proceedings Proceedings of the 2nd International Conference on Applied Science and Technology (ICAST'17), 1891*, Kedah, Malaysia, pp.1. https://doi.org/10.1063/1.5005410

IAB. (2016). *A global perspective of mobile commerce* [Online]. New York City, NY. https://www.iab.com/wp-content/uploads/2016/09/2016-IAB-Global-Mobile-Commerce-Report-FINAL-09 2216.pdf. (Accessed 22 March 2018).

Ibukun, E., & Daramola, O. (2015) A systematic literature review of mobile cloud computing. *International Journal of Multimedia and Ubiquitous Engineering, 10*(12), 135-152. https://doi.org/10.14257/ijmue.2015.10.12.15

Kim, S., & Kim, J. (2016) Determinants of the adoption of mobile cloud computing services. *Information Development, 34*(1), 44-63. https://doi.org/10.1177/0266666916673216

Kivunja, C., & Kuyini, A. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5), 26-41. https://doi.org/10.5430/ijhe.v6n5p26

Lee, W., & Wong, L. (2016). Determinants of mobile commerce customer loyalty in Malaysia. *Procedia-Social and Behavioral Sciences, 224*, 60-67. https://doi.org/10.1016/j.sbspro.2016.05.400

Lu, X., Qu, Z., Li, Q., & Hui, P. (2015) Privacy information security classification for internet of things based on internet data. *International Journal of Distributed Sensor Networks, 11*(8). https://doi.org/10.1155/2015/932941

Mishra, A., Medhavi, S., Mohd, K., & Mishra, P. (2016). Scope and Adoption of M-Commerce in India. *International Journal of Advanced Research in Computer and Communication Engineering, 5*(8), 231-238.

Mollah, M., Azad, M., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications, 84*, 38-54.

https://doi.org/10.1016/j.jnca.2017.02.001

Nilashi, M., Ibrahim, O., Reza Mirabi, V., Ebrahimi, L., & Zare, M. (2015). The role of security, design and content factors on customer trust in mobile commerce. *Journal of Retailing and Consumer Services, 26*, 57-69. https://doi.org/10.1016/j.jretconser.2015.05.002

Noor, T., Zeadally, S., Alfazi, A., & Sheng, Q. (2018). Mobile cloud computing: Challenges and future research directions. *Journal of Network and Computer Applications, 115*, 70-85. https://doi.org/10.1016/j.jnca.2018.04.018

Plateaux, A., Lacharme, P., Vernois, S., Coquet, V., & Rosenberger, C. (2018). A comparative study of card-not-present e-commerce architectures with card schemes: What about privacy?. *Journal of Information Security and Applications, 40,* 103-110. https://doi.org/10.1016/j.jisa.2018.01.007

Ponto, J. (2015). Understanding and Evaluating Survey Research. *Journal of the Advanced Practitioner in Oncology, 6*(2), 168-171, March. https://doi.org/10.6004/jadpro.2015.6.2.9

Rajhashyamala, M., Thomas, A., Vaishnavi, A., & Manoj, K. (2017) The survey on mobile computing and its applications. *International Research Journal of Engineering and Technology, 4*(1), 1259-1262.

Sultan, M., Khan, H., & Khan, S. (2016). Studying the impact of point of differences of m-commerce over e-commerce: Are they really significant in providing edge to M-Commerce in developing areas of the world: Evidence from the customers of Karachi City'. *International Journal of Scientific and Research Publications, 6*(10), 401-407.