Shirazi and Iqbal *Journal of Cloud Computing: Advances, Systems and Applications* (2017) 6:22
DOI 10.1186/s13677-017-0093-0

Journal of Cloud Computing: Advances, Systems and Applications

RESEARCH Open Access

Community clouds within M-commerce: a privacy by design perspective

Farid Shirazi[1*] and Amna Iqbal[2]

Abstract

The paper establishes the link between community clouds and m-commerce. The research questions attempt to provide an understanding of the various shopping domains and their convergence through mobile devices. In addition, insight is provided into the development and growth of mobile trends within the context of m-commerce and the cloud. This enables analysis of the Privacy by Design (PbD) framework and uses it to evaluate the next generation of m-commerce designs. This is followed by a discussion of the current issues based on the PbD framework, as well as offers of a solution framework to address the relevant challenges.

Keywords: Community clouds, M-commerce, Security, Privacy, Privacy enhancement technologies, Privacy by design

Introduction

E-commerce, once a new and emerging field, has gained massive popularity and is on a trajectory for continued growth, particularly in the area of mobile commerce. The term m-commerce refers to the availability of commerce capabilities through wireless devices. It can be considered shopping online and on-the-go. Due to the wireless aspect of m-commerce associated with the portability of smartphones, there is a wider range of shopping capabilities that can be available [1]. Parallel with the expansion of e-commerce in general and m-commerce in particular, we have witnessed an exponential growth of cloud computing technology.

Cloud computing refers to the availability of resources through an on-demand system. Here, the emphasis is on shareability, efficiency, and cost reduction. The cloud is known by various terms, such as "on-demand computing, utility computing, or pay-as-you-go computing" ([2], p.84). It allows applications to execute faster and accommodates a wide variety of projects in a timely manner. Additionally, "cloud computing is a distributed computing paradigm that focuses on providing a wide range of users with distributed access to scalable, virtualized hardware and/or software over the internet" ([3], p.42). Andrew McAfee, in the Harvard Business Review (November 2011) article *What every CEO needs to know about the cloud*, refers to cloud computing as "a sea change—a deep and permanent shift in how computing power is generated and consumed" ([4], para 5).

According to [5] the cloud model has three essential service models namely, Software-as-a-Service (SaaS), Platform-as-a-Service and Infrastructure-as-a-Service, and four deployment models. The deployment models are the actual implementation of cloud in form of private, public, hybrid, and community clouds. The latter is designed for exclusive use by a specific community of organizations that have shared missions for addressing and developing solutions that impact consumers and businesses through m-commerce technology, and concerns (e.g. security requirements, policy, and compliance considerations). The community cloud may be owned, maintained, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises [5].

It is expected that cloud computing enables organizations to expand or contract on demand and provide services at reduced cost. By migrating to such solutions, organizations are not only able to reduce capital and operational expenditures but also to create and sustain a global competitive advantage. According to Gartner report [6] cloud services accelerated workload deployments from weeks to days to minutes, and technologies like containers

* Correspondence: f2shiraz@ryerson.ca
[1]Ted Rogers School of Information Technology, Ryerson University, 350 Victoria Street, Toronto, ON M58 2K3, Canada
Full list of author information is available at the end of the article

Springer Open

© The Author(s). 2017 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

are accelerating scaling and provisioning to seconds. As such, it is not surprising to see that one of the most successful e-commerce businesses such as Amazon was able to successfully integrate its business into cloud. Amazon was also among the first companies to offer commercial cloud services through the introduction of Amazon Web Services (AWS) in 2002 and its Elastic Compute Cloud (E2C) service in 2006. The latter provides a commercial service through which users can rent computers and related storage and run their own applications [7]. In addition, architectures like "serverless" programming (supported by AWS Lambda) enable more agility for those applications designed to be event-driven and real-time [6] such as e-commerce applications. According to [4], "As the cloud grows and matures, its vendors will continue to innovate and to differentiate their offering" ([4], para 49).

It is also important to note that although cloud solutions provide many advantages, there remain serious challenges ahead including but not limited to security and privacy issues associated with the introduction of new technology.

This study focuses on a thorough overview of privacy issues associated with m-commerce, the constituents of privacy, and the perceptions of privacy. It offers an overview of two existing models namely, Privacy Enhancing Technologies (PETs), and Privacy by Design (PbD). The latter allows for an understanding of the integration of other technologies within the framework of privacy. Therefore, the privacy by design framework is not to be interpreted solely as compliance with a technology-oriented regulation [8]. Rather, it should be viewed as instilling responsibility for the development and execution of data processing systems [8] such as services offered by cloud. Because PETs are being replaced by the privacy by design concept, the focus has been on the design stages [8]. As mentioned by [8] systems should be built from a privacy perspective, beginning at the design stage.

The goals and objectives of this study can be summarized through the research questions that follow:

1. What are the most significant factors impacting privacy and the rise of the use of mobile devices within cloud and m-commerce portals?
2. How can the security and privacy needs and challenges within the specific context of mobile devices be addressed?
3. Do mobile apps join these various shopping domains?
4. How likely are the mobile trends to continue in the future?

The paper will also evaluate shopping behavior in various domains within the context of mobile devices and cloud. The focus on this topic is due to its surging popularity and development within the e-commerce portals. The increasing popularity and developments within the e-commerce portals lead to the need to address requirements for privacy and security. This paper will draw on extensive research from varied areas such as statistical approaches, news reports, academic sources, and databases. The research will assist in understanding the interaction of privacy with other components of a system/business, the factors impacting privacy, the challenges faced by privacy, and the possible ways that the challenges and their impacts can be reduced. This paper will also focus on keyword analysis, and will look at shopping behavior in various domains within the context of the mobile device.

M-commerce, cloud and privacy: A literature review

The existing literature pertains to research based on the emergence of m-commerce, the cloud, the development of online portals, and the inclusion of mobile devices [9–12]. It provides insight into the classification of m-shopping within the scope of online distribution channels and advanced technology for in-store shopping. Mobile commerce considers the integration of traditional business with distributed commerce [13]. There has been an inclination towards mobility, and this has led to the increase in ubiquitous and smart mobile devices [14]. This increase has resulted in improved communications performance [15]. The performance improvement is visible for example in the number of ways that mobile agents can be used to search and sell products in malls [16].

There are differences between cloud computing and mobile cloud computing. The latter offers the services of the former within the realm of mobile devices. Mobile cloud computing is defined as the "running of an application on a remote resource rich server" ([2], p.87). The authors mention that, the issues in mobile cloud computing include: "operational level issues; end user level issues; service and application level issues; privacy, security and trust, context-awareness, data management" ([2], p.88).

As we discussed earlier, within the cloud, there are subdivisions of public, private, hybrid and community. While private clouds pertain to services (hardware and software) that are restricted to an organization, the public cloud offers services (hardware and software) to the general public. Both public and community clouds belong to the same collaboration type, however, from security perspectives, the latter provides a higher level of security [17].

There is no doubt that cloud computing has an impact on the manner in which the purchase and development of IT hardware occurs, and it has potential advantages such as innovation and cost effectiveness [3]. This is enabled by the customizable offerings of the cloud, for example, in the service models of cloud computing, such as IaaS, PaaS and SaaS. IaaS is "the provision processing, storage, networks…

the consumer is able to deploy and run arbitrary software" ([3], p.21). Currently, the consumer does not participate in the management or control of the cloud infrastructure. In PaaS, there is an option for creation and modification of applications. Specifically, it refers to the leveraging of a development language for the creation of applications and utilization of the cloud service [3]. In contrast, SaaS refers to the consumer's ability to use the provider's applications [3]. These applications are present in the cloud's infrastructure. All of the aforementioned applications have a considerable impact on business [3, 17–19].

There are a plethora of factors that may impact the integration of cloud computing within businesses. Within the specific realm of small- and medium-sized enterprises, these factors can range from cost estimates, ease of use, learning curves, and the perceived and actual needs and expectations of the businesses. In addition, the issues of diverse mobile operating systems (e.g., mac and incompatibility) must also be considered.

Thus, while there is an abundance of mobile-oriented applications [2], there are still many untapped areas of growth. These include applications that span across diverse categories such as news, business, games and entertainment [2].

The increase in m-commerce has opened the debate on privacy. Currently, the perception of e-visitors regarding their privacy in e-stores is poor [19]. E-visitors are dependent on e-merchants for protection of their data and for compliance with the mechanisms of flexibility, external regulation, and information practices [19]. There are numerous other methodologies that consider the extension of the traditional commerce model for the purchaser relative to their personal information [20].

Privacy issues are predominant in technology such as e-commerce, big data and cloud computing [21]. The latter provides immense resources for cloud users to manipulate complex datasets in applications [21]. However, it also endangers privacy due to breaches [21]. The key lies in the balance among cost effectiveness, scalability, flexibility and privacy preservation [21]. Security is also of significance within context of m-commerce and cloud, and this takes into account the development of mobile technology for enhancing usability and increasing security [22]. However, this may not always be possible due to implementation challenges, including a lack of economic incentives and a lack of acceptance by PbD end users in commerce [8, 23]. In addition, the research highlights the following:

First, emphasis is placed on mobile marketing, retailing methodologies with a specific focus on purchasing patterns pertaining to mobile devices and consumer technology traits. Mobile marketing is performed through mobile shopper marketing [9–11], which is the merging of mobile marketing and shopper marketing. The increase in mobile-mediated transactions and the factors that impact the consumers' intention to adopt m-shopping are observed through additional variables, specifically, compatibility (CO), perceived enjoyment (PE) and perceived cost (PC) in the original technology acceptance model (TAM) [9, 10, 24].

Second, the relevant literature delves into the history and the development of m-commerce. This provides an understanding of the increase in demand for mobile applications and e-commerce websites. This shows that commerce will no longer be a luxury, but will become a necessity. The literature provides insight into the achievement of wireless secure e-commerce operations (see for example [25, 26] for more details).

Third, the literature discusses the global trading environments offered by e-commerce and the link between e-commerce and holidays, with examples of holidays causing an increase in sales. This facilitates a discussion of mobile commerce's recommendation model that is both personalized and commercialized. This discussion provides insight into large data processing and cloud computing for mobile business [27].

Fourth, the literature discusses mobile privacy and security concerns, specifically PETs and PbD. Within the context of m-commerce and the cloud, the analysis of the Privacy by Design (PbD) framework and its use for evaluation of the next generation of m-commerce design is discussed. Additionally, the research focuses on the prevalent issues and challenges of privacy in m-commerce and the cloud.

Finally, the existing literature shows the current limitations of the buying experience for consumers that can be rectified by (i) the emergence of new technology; (ii) the engagement of customers; (iii) an increase in m-commerce applications; (iv) addressing the issues pertaining to privacy and security; (v) growth in elements of trust as well as the convergence of communications within e-commerce; and (vi) on features such as mobility, sociability and autonomy.

Privacy

As mentioned above, privacy issues are predominant in technology such as e-commerce, big data and cloud computing [21]. The growth of wireless communication has led to the emergence of a range of handheld devices, such as PDAs, mobile phones, palm computers [28], and wearable computers such as smartwatches. This growth has highlighted the issues of privacy. According to [29] recent works on cloud privacy have mainly focused on evaluating the reliability of the Cloud Service Provide (CSP) in terms of its security and data privacy measures and its compliance with its SLA [29]. However, little work has been done to investigate the privacy issues from an architectural design perspective. For example, there are several important aspects of privacy, including the incorporation of privacy protections within a

business organization and the maintenance of substantial data management procedures for the duration of the cycle of products/services [30]. According to [31], within the realm of privacy, there are numerous soft computing techniques that must be considered, which lead to the contextual awareness of the principles. These include the development of reliable procedures that allow user access to services [31]. In addition, the access is delegated in conjunction with traditional methods such as cards and personnel numbers [31]. This is expanded through the development of algorithms that consider multiple biometric systems [31]. Other aspects of privacy build on Privacy Enhancing Technologies (PETs) [30]. PETs have defined the context of Privacy by Design (PbD), as the promotion of consumer privacy within organizations is important at every stage of product/service development [30].

The following sections contain highlights of PETs and PbD frameworks.

The PETs privacy framework

The concept of PETs is complex. It considers new as well as emerging systems. The addition of PETs onto existing systems leads to an impact on system functionality regarding privacy [30]. Because of this, PETs have often been viewed as almost an afterthought by users [30]. Additionally, there is a lack of awareness of the differences between PETs and PbD [30], as seen in the often unnoticed differences between the PETs and PbD paradigms [30]. There are several ways that these differences can be addressed, including the application of formal methods to facilitate architecture language and logic [18].

PETs are defined as privacy-enhancing technologies that attempt to reduce privacy risks, minimize data held on individuals, and empower individuals to control their own data [32]. However, the integration of several PETs components is challenging because of the implementation of multiple technologies [18]. In this manner, PbD becomes directly embedded into measures pertaining to the PETs [33]. Such technologies then consider communications, privacy in databases, data mining and information retrieval [33]. Cavoukian [34] argues that while PETs were seen as the solution to ICT privacy concerns, we need a more substantial approach for today's business — extending the use of PETs and their successor PETs-Plus to a full functional approach as described by the PbD framework. Rubinstein [30] notes that despite similarities, PETs and PbD are not identical frameworks. Their differences according to [30] are as follows: PETs are applications or tools that address a single dimension of privacy, such as anonymity, confidentiality, or control over personal information. In addition, PETs are added onto existing systems, sometimes as an afterthought by designers and sometimes by the end-users. In contrast, PbD is a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture (see [30] for more details). The intrinsic value of this design approach lies in its ability to adapt to any technology or product, including cloud computing and m-commerce as discussed in this paper.

The PbD framework

PbD framework contains seven fundamental principles such as: Proactive not Reactive; Privacy as the Default Setting; Full Functionality; End-to-End Security; Visibility; Transparency; and User Privacy and Privacy Embedded into Design. The latter in particular is an important part of this study. The PbD framework offers an approach that is characterized by a proactive privacy measures rather than reactive ones, it assures that all stakeholders whether the business practice or technology involved, operate according to the stated promises and objectives and subject to independent verification [34]. PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults. This includes building privacy-oriented features, earlier implementation of relevant controls, and diversity of the processed data [33]. There are several opportunities that can apply the development of PbD, including the integration and accounting of PbD for the Internet of Things (IoT) [35].

There are several areas where PbD has been used to elicit privacy requirements. This is accomplished by adherence to the framework of [34] and considering a proactive, preventative, and transparent approach [35]. The current self-regulation has undergone criticism because of its inadequacy for privacy security [17]. This has led to the drive for PbD incorporation within technical systems, leading to a higher accountability of business practices and integration within the design and the network [32]. Therefore, PbD becomes a process rather than a set of principles [32].

PbD provides several opportunities for development and addressing the challenges associated with privacy designs in software. There are numerous privacy and security challenges arising from malware and vulnerabilities [36]. These include issues pertaining to authorization/authentication, broken cryptography, improper session handling, and inadequate server side controls [36]. PbD in conjunction with an understanding of an application's context would enable issues pertaining to the protection of user privacy to be addressed [37].

PbD offers extensive functionality, specifically for the safeguarding of privacy [38]. The PbD system can also be seen as multi-disciplinary, considering various dimensions such as technology, the user perspective, design and organization [38], among others. These

dimensions relate to awareness of the privacy risks of incorporating IT system applications with accountable business practices into the physical design and networked infrastructure [34].

The size of cyberspace has been increasing, and this has had an impact on technology as well. Specifically, cyberspace's regulations are increasingly and directly impacted by the development of technology [39]. The PbD framework would benefit by being supplemented by technology and organizational procedures [38]. These procedures would be focused on a privacy first approach that considers the protection of privacy in the development of technology [38]. The concept of PbD can be propagated by collaboration between IT system administrators and system developers, with the goal of internalizing data protection [8]. This may facilitate organizational changes that consider both technology and organizational measures [8].

The differences in and the discussion of PETs and PbD pave the way for the industry challenges, as described below.

Industry gaps and challenges in privacy

There are numerous industry challenges related to privacy. First, there has been a push towards automation to further privacy principles. This is seen in the increase in the number of automated decisions [31]. However, there must be compliance with the legal requirements of a region, and this responsibility is placed on the data collectors [31]. This provides the distinction between the data owners and the cloud service providers. Since there are differences within their trust domains, the protection of data privacy is dependent on encryption and effective database utilization [40].

There are numerous issues that must be considered for the implementation of m-commerce with business integration. These include the application of business process management to m-commerce with the consciousness of privacy, as well as solving any privacy challenges [41]. While there are numerous privacy challenges arising from m-commerce, the uniqueness of some of its attributes allows for convenient operations and interaction within wireless environments [41].

The protocols pertaining to m-commerce's privacy domain also enable its security protection and enhance its functionality [41]. Therefore, the concern is extended to both perspectives of m-commerce: one that views it as an extension of e-commerce and the second that views it as distinct from e-commerce [42]. The first is called the extension view, and the second is called the uniqueness view [42]. The latter allows for the privacy challenges of m-commerce that are based on the uniqueness view [42]. Other privacy-enhancing mechanisms include people-centric sensing (PCS), which enables malware detection and efficient management [43]. Therefore, the PbD paradigm considers a range of factors such as customers' concerns, the acceptance of technology, and organizational security and privacy practices [44]. This results in shared responsibility for privacy. Privacy policies then become the responsibility of varied departments and organizational levels [44].

Other instances are seen in MCH, which is the mobile crowdsourcing network focused on the integration of mobile capabilities with crowdsourcing [45]. In this manner, there is an application of human involvement with mobile devices [45]. Confidentiality and user privacy are important parts of PETs [46]. The combination must consider efficiency, usability, and privacy [23]. This is evident in the mobile agent security problem where greater emphasis is required on encryption [47]. There are costs associated with information privacy. Previously, these costs were quite high; however, they have decreased over the past several years [48]. As mentioned by [49], there has been an increased focus on security, cryptography and privacy when it comes to the future of mobile communications.

Shopping behavior

There are varied and evolving advantages of m-commerce. These range from flexibility, portability, and ease of use, to the availability of shopping options, coupon availability, and ease of redeeming coupons. As such, m-commerce increases consumer demand, and consequently the profits for businesses. A portion of the reason is continuous consumer contact, and so the focus is placed on consumer engagement [50]. This facilitates the linkages with consumer shopping behavior.

M-commerce has had a significant impact on shopping behavior. In general, e-commerce has transformed the business sphere since its emergence in the 1990s [24]. This is apparent across aspects such as retail, shopping and customer behavior. M-commerce has gained popularity through the availability of electronic payment systems and diverse web services. The former work through networks and cellular-service providers [51], and the latter are accessibility oriented and lighter-weight smartphones and laptops [52].

M-commerce has huge potential for growth. According to eMarketer, "m-commerce's rapid growth is primarily coming from smartphones" and smartphones will surpass the sales of tablets for the first time in 2017 and comprise nearly 50% of all retail m-commerce sales [53]. In particular, the emerging markets show substantial potential for m-commerce service providers [24]. However, this potential cannot be analyzed easily, as it is subject to a range of factors. For example, the services offered by mobile providers allow pattern prediction and have added popularity to m-commerce [24, 52].

Theoretical framework and data analysis

The theoretical framework of this study considers concepts, variables, and relationships pertaining to mobile devices within e-commerce, and the corresponding privacy and PbD challenges. The research study is inclined towards the inductive method, in keeping with the continuous development of privacy, and the plethora of factors impacting privacy, security and usability trends. As the use of mobile devices is fairly new, there is a possibility of new observations from the data. A variety of research methods are incorporated to perform data analysis.

In this exploratory study, we conducted two sets of data analyses on existing literature regarding m-commerce, community clouds and data security and privacy. A total of 89 relevant articles were analyzed. We conducted our data analysis through five unique steps. In step 1, each article was assigned a unique identification code. In step 2, each article was imported as an Adobe PDF document into NVivo 10 data analysis software, and the source articles were then coded using the following categories: a) terms used to describe m-commerce - technology, keywords and the associated frameworks; b) statements regarding e-commerce privacy and security issues; and c) statements regarding m-commerce cloud computing privacy and security issues. In step 3, a textual reproduction of all of the empirical observations was generated. From the lists of extracted keywords from reviewed articles shown in Appendix A, we were able to identify 158 unique keywords. We were then able to export those keywords into Microsoft Excel tables for further analysis. In step 5, from the 158 unique keywords, we were able to sort and categorize 148 into eight different categories as shown in Table 1.

The data in Table 1 can be visualized via the bar chart in Fig. 1.

Table 1 Frequency Analysis

Categories	Highest Frequencies	Percentage
Mobile	40	19.04
Platforms	22	10.47
Consumer	17	8.05
Ecommerce	15	7.14
Cloud	14	6.66
Retail	14	6.66
Privacy/Security	14	6.66
Marketing	12	5.71

Data observations

Our data observations from the extant literature show that in general, mobile was a significant occurrence, with appearances in the areas of shopping, commerce, communications and locations. It also overlapped in the marketing and cloud categories, through the use of keywords such as mobile marketing and mobile cloud computing. Mobile shopping was used interchangeably with m-shopping, as was mobile commerce with m-commerce and mobile e-commerce. Additionally, there was little or no emphasis on mobile security and privacy.

Within cloud, the primary focus was on the types of clouds, security, and the business components. The retail category was expansive and covered a range of areas, considering the perspectives of the retailer, the online retailer, and vendors. In doing so, the focus was on profits and the payment ecosystem.

The groupings for privacy/security revealed the associated jurisdiction and regulation. The conceptual and miscellaneous categories held keywords that could not be solely and primarily placed in the other categories. However, they were significant in understanding the context and the discussion of this study. The keywords related to privacy and security research are shown in Table 2.

Within the context of m-commerce, Table 2 highlights the following:

(i). The emphasis on privacy is greater than that on security.
(ii). There are numerous commonalities between privacy and security.
(iii). There are security-specific solutions; however, privacy is developing at a faster pace.

Finally, one of the notable issues that emerged from our literature review is that we could not locate any keywords representing community clouds with m-commerce (see Table 3 in Appendix).

Proposed models

With regards to IT adoption, one of the prominent e-commerce models discussed in literature is the Technology Acceptance Model (TAM) [54, 55] and its extension [56]. This theory consists of four direct determinants; "*Perceived Usefulness*", "*Perceived Ease of Use*", "*Intension to Use*", and "*Usage behavior*". According to [57] in *Exploring the Factors Influencing the Adoption of Mobile Commerce*, the perceived usefulness and perceived ease of use are two key determinants of technology adoption. The author argues that while TAM is a useful model for predicting user's intention to adopt a new technology, incorporating the perceived behavioral control, drawn from Theory of Planned Behavior (see [58] for more details), provides a better explanation for the user intention to adopt new applications and services such as m- commerce. According to [46], the prevalent m-commerce model is shown in Fig. 2.

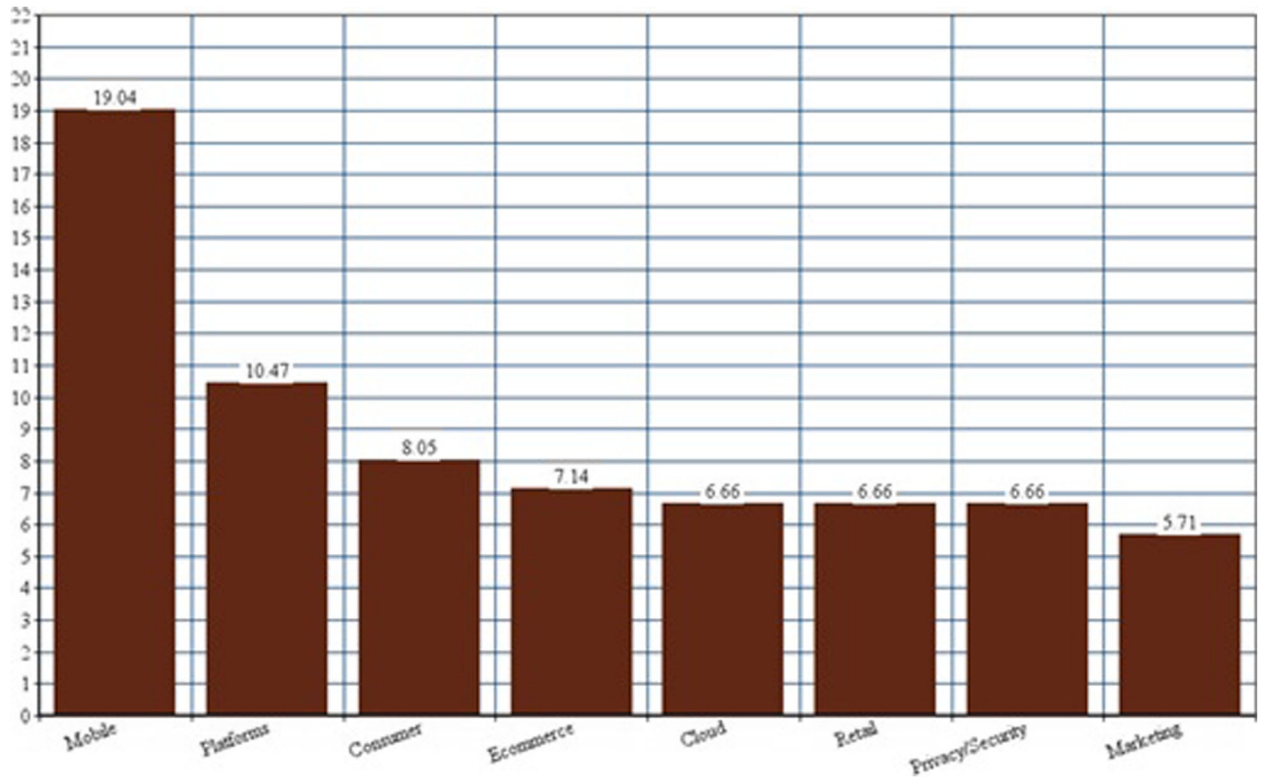

Fig. 1 A chart view of frequencies

Li [59] argues that TAM's fundamental constructs in determining the acceptance and use of technology may not fully reflect the user's behavior toward newly emerging technology like e-commerce including the Internet Banking and/or the m-commerce. The author stresses the fact that the risk perception associated with security and privacy concerns over the Internet has been a common and widely recognized deterrent to e-commerce acceptance. This claim is confirmed by our study summarized in Table 2. As such, security and privacy along with the usability of a system, as depicted in Fig. 4a play an important role in customer's acceptance of new technology, in particular the e-commerce. The current interaction of privacy, security and usability as mentioned by [59] is shown in Fig. 4a.

The aforementioned discussion on mobile commerce and clouds has highlighted the gaps in security and privacy for businesses. These issues must be balanced in conjunction with accommodation for growth and collaboration. This is where the concept of community clouds can be beneficial. Community clouds are defined as a service provided to a defined number of individuals that is managed and governed by a third-party provider [60].

Community clouds are cost effective and assist users with security and privacy. They have similarities with private clouds, except that the availability of resources is guided by security and privacy protocols and is "exclusive to two or more organizations" ([3], p.25). The modes of improvement for community clouds include reducing costs and addressing the "fixed amount of bandwidth and data storage shared among all community members" ([3], p.25).

Community clouds are used when there is a construction and sharing of "cloud infrastructure… requirements and policies" ([61], p.879). There is also the provision for the cloud infrastructure to "be hosted by a third-party provider or within one of the organizations in the community" ([61], p.879). The advantages of cloud computing can range from "easy management, cost reduction, uninterrupted services disaster management, and green computing" ([61], p.879) to high availability [62]. All of these enable community clouds to be a viable option to address the needs of m-commerce in conjunction with security and privacy.

The model shown in Fig. 2 does not address the impact, positioning, and usefulness of community clouds. Specifically, this study links the community cloud to m-commerce as depicted in Fig. 3. Doing so will enable understanding of the cloud providing for all customers under one consolidated platform rather than tiny applications on different platforms. This is through the community/industry cloud, which co-locates all e-commerce or selected e-

Table 2 Observations of Privacy and Security

Privacy-Oriented	Security-Oriented
Data Privacy	Security (5)
Privacy (11)	Intrusion Detection
Security and privacy of mobile VoIP apps	Security and privacy of mobile VoIP apps
Biometric identification	Biometric identification
Privacy-by-design (15)	Data Security
Identity management	Identity management
PETs	Security Perception
Privacy protocols	
Privacy requirements	
Privacy principles	
Privacy impact assessment	
Revocable privacy	
Data protection (3)	
Privacy concerns	
Trust (2)	Trust (2)
Privacy preservation	
Information privacy	
Privacy concerns	
Concerns for Information Privacy	
Data Protection Regulation	Data Protection Regulation
Privacy-enhancing technologies	
Privacy impact assessment	
Privacy Aware	

commerce applications under on one platform. In addition, it enables the research of mobile applications for m-commerce from the perspective of client accessibility.

The inclusion of the community cloud allows for linking with perceived usefulness and ease of use. In addition, it allows for personal innovativeness, through openness to creativity and change. Ultimately, these attributes allow users to ease into their intention to adopt. Figure 4b shows the integration of the PbD framework into the legacy framework of privacy, security and usability (see Fig. 4a) as described by [61, 63]. This integration highlights the vital links between privacy, security and usability in building an organization's credibility and trust [64].

The updated model considers the dynamic nature of privacy. In addition, it addresses the need for flexibility, adaptability and transparency [65] in the process. This facilitates a richer and smoother user experience. It establishes the required accountable business practices with the commitment to customers' relationships as related to privacy and trust in mobile cloud computing. As argued by Vanderhoof [66], addressing privacy can be done via socio-cultural solutions, i.e., considering the user and the system. This would not only facilitate greater trust between the user and the system [66], but also the organization's commitments for protecting privacy of customers and their personal information.

Moorman et al. [67] state that commitment is synonymous to value in a relationship. In this context, relationship commitment and trust are not only important variables in marketing relationships [68, 69] but also are key mediating variables in these relationships [70]. In addition, relationship commitment positively influences acquiescence, whereas trust influences acquiescence only through relationship commitment. As such, relationships are built on the foundation of mutual commitment [71], and trust exists when one party has confidence in an exchange partner's reliability and integrity [70]. When both commitment and trust are present, they produce outcomes that promote efficiency, productivity, and effectiveness. In short, commitment and trust lead directly to cooperative behaviors that are conducive to relationship marketing [70]. Finally, the integration of PbD into the mobile community cloud, as argued by [34], advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, assurance of privacy offers organizations a suitable mode of operation for building trust with their customers.

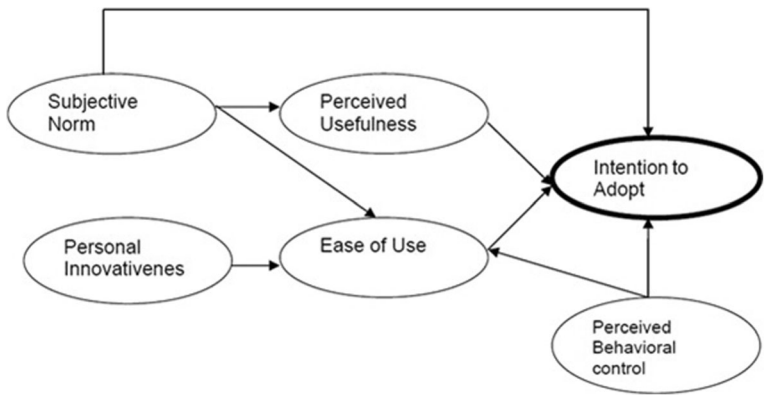

Fig. 2 Mobile Source Adoption. Source: [46]

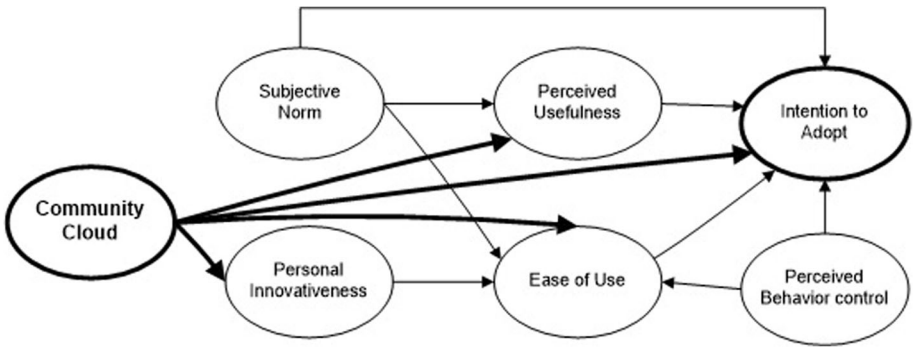

Fig. 3 The m-commerce cloud adopted from [57]

Conclusion

The above discussion highlights the importance of the placement of community clouds within industry. It has numerous benefits, including addressing incompatibility, trust (application, infrastructure), ease of use, and cost effectiveness.

There has also been encouragement for e-commerce to focus on mobile compliance and compatibility within a range of platforms. This is due to the multitude of advantages for mobile internet that allow the cloud to have constant access to resources. The trends are expected to continue as "mobile commerce traction will continue its climb; for retailers, the money is in the mobile Web, not the app; optimized mobile checkout will be a top priority; and physical stores will support the mobile surge" [72].

As discussed above, the community cloud is a collection of industry standards. There is an existing lack of standards (which is limiting user-friendly mobile internet, wireless access, and ubiquitous access to resources (update, modify, downloads)). By focusing on industry standards, community clouds define their niche and show their potential positive impact to businesses, consumers, and the industry as a whole. It will enable the industry to be more cohesive, allow better business models, and allow for smoother mobile commerce experiences. This would increase the demand for businesses and allow more choices for consumers.

Addressing privacy can be done via socio-cultural solutions, i.e., considering the user and the system [73]. This would facilitate greater trust between the user and the system. Therefore, trust cannot be seen as permanent but instead has to be continually renegotiated [73]. For confidence and the protection of information, a combination of technology and business policies is needed [66]. There has been an increase in the concern towards privacy, especially within the context of data analysis [74]. Privacy by design enables the development of a technology framework that addresses the privacy challenges [74]. The aforementioned background, discussion, data analysis, and proposed model have highlighted the interaction among privacy, security, and adaptability.

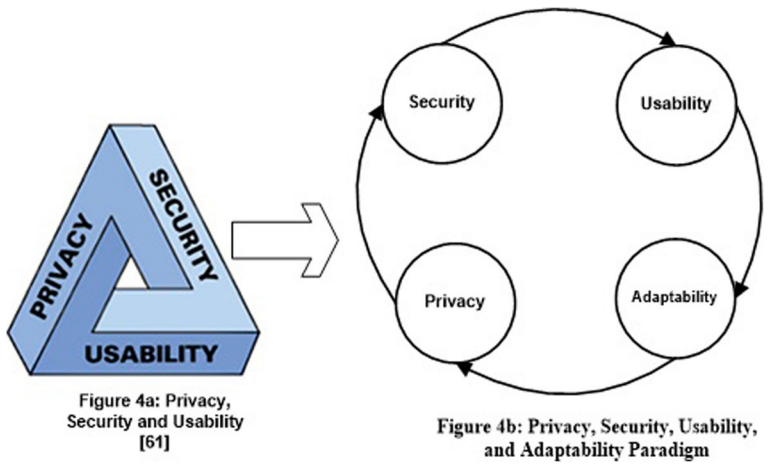

Figure 4a: Privacy, Security and Usability [61]

Figure 4b: Privacy, Security, Usability, and Adaptability Paradigm

Fig. 4 Privacy, Security, Usability and Adaptability

Appendix

Table 3 Keyword Categories

Categories	Keywords Included	Combined Frequencies
Mobile	m-shopping; mobile shopping; mobile purchasing satisfaction; mobile shopping adoption; mobile commerce; mobile content; mobile communications; mobile revenue models; mobile ecosystem; m-commerce; mobile services; mobile locations; mobile accessing sequences; mobile ecommerce; mobile; mobile payments; mobile multi agent systems; mobile marketing; mobile bidders; mobile cloud computing.	3 + 4 + 1 + 1 + 6+ 2 + 1 + 1 + 1 + 5+ 1 + 1 + 1 + 6 + 1+ 1 + 1 + 1 + 1 + 1 =40
Cloud	Cloud computing; community cloud; business component of cloud computing; public cloud; private cloud; hybrid cloud; cloud community; cloud security; mobile cloud computing; SaaS.	4 + 2 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1 =14
Retail	retail; multi-channel retailing; online retail; online retailer; purchases; vendor; profitable; payment ecosystem; cross-sell; coupons; retail industry; supply chain visibility.	2 + 1 + 2 + 1 + 1+ 1 + 1 + 2 + 1 + 1+ 1 =14
Marketing	Mobile marketing; shopper marketing; digital marketing; marketing holiday; business to business; global market; persuasion; database marketing; email marketing; mobile marketing; coupons.	1 + 1 + 1 + 1 + 2+ 1 + 1 + 1 + 1 + 1 +1 =12
Ecommerce	Ecommerce; ecommerce risks; electronic commerce; ecommerce servers; coupons.	10 + 1 + 2 + 1 + 1 =15
Consumer	Involvement; consumer decision making; consumer traits theory of planned behavior; consumer behavior; customer segmentation; personalized information; recommendation model; business to consumer; customer loyalty; consumer behavior.	1 + 1 + 1 + 1 + 1+ 2 + 3 + 3 + 2 + 1 +1 =17
Platforms	Smartphones; traditional or wireless; stationary or mobile; software agents; access points; traffic; 3G mobile; android development; mobile client; wireless interactivity; mobile devices; wireless; system resources; digital devices services; wireless devices; traffic characterization; interactive digital television; digital products.	1 + 1 + 1 + 2 + 1+ 2 + 2 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 =22
Privacy/Security	Data encryption; cyber jurisdiction; internet jurisdiction; internet regulation; trust; security; mass customization; privacy; data mining; identity management; cloud security.	1 + 1 + 1 + 1 + 2+ 1 + 2 + 1 + 1 + 1+ 1 + 1 =14
Conceptual	Technology Acceptance Model (TAM); multiple regression analysis; WOM Age Satisfaction Entertainment and Subjective norms; E-CWE; repository; WAP; k-means; RFID; semantic reasoning; collaborative filtering; flipkart; common floor; xiaomi; BDI agent; hierarchical regression analysis.	3 + 1 + 1 + 2 + 1+ 6 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1 =23
Miscellaneous	Classification framework; literature; c2b; switching behavior; push pull mooring; synergy effect; technology; luxury; agent based environment; reception; environment issues; artificial bee colony; importance constraints; new trend; pipeline entity; pipeline characteristic; pipeline object; architectural model; network challenge; information and communication technology; voice recognition; user perceived response time; fuzzy logic; network bandwidth; throughput bandwidth; traditional model; convergence; self-familiarity and web servers; user interface; text message; HDFC bank; axis bank; airtel money; intelligent process; collaboration; task; SPPR; STPPR; applications; architecture; pervasive network; task offloads; MTA.	1 + 2 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 + 1 + 1+ 1 + 1 + 1 =39

Acknowledgments
We would like to thank our anonymous reviewers for the constructive comments and suggestions for improving the quality of this manuscript.

Funding
Not applicable.

Authors' contributions
FS provided the main idea of the paper, designed and integrated PbD framework into the final framework developed by AI. AI did an extensive literature review, data and regression analysis. Based on this analysis, AI developed a framework for m-commerce adopted from Bhatti (2007) as depicted in Fig. 3. FS finalized the paper by integrating PbD into the m-commerce model. Both authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1]Ted Rogers School of Information Technology, Ryerson University, 350 Victoria Street, Toronto, ON M58 2K3, Canada. [2]Ted Rogers School of Management, Ryerson University, Toronto, Canada.

Received: 28 March 2017 Accepted: 24 October 2017
Published online: 02 November 2017

References

1. Kourouthanassis EP, Giaglis MG (2012) Introduction to the special issue on mobile commerce: the past, present, and future of mobile commerce research. Int J Electron Commer 16(4):5–17
2. Fernando N, Seng L, Rahayu W (2013) Mobile cloud computing: a survey. Futur Gener Comput Syst 29:84–106
3. Goyal S (2014) Public vs private vs hybrid vs community- cloud computing: a critical review. I.J Comput Network Inf Security 3:20–29
4. McAfee A (2011, November) What every CEO needs to know about the cloud. Harv Bus Rev Retrieved from: https://hbr.org/2011/11/what-every-ceo-needs-to-know-about-the-cloud
5. Mell P, Grance T (2011) The NIST definition of cloud. Computing Retrieved from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
6. Gartner (2016). When Private Cloud Infrastructure Isn't Cloud, and Why That's Okay. Retrieved from: https://www.gartner.com/doc/reprints?id=1-3Y0I7E8&ct=170414&st=sb
7. Harauz J, Kaufman LM, Potter B (2009) Data security in the world of cloud computing. IEEE Security & Privacy 7:61–64
8. Koops B, Leenes R (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. Int Rev Law, Comput Technol 28(2):159–171
9. Groß M (2015) Mobile shopping: a classification framework and literature review. Int J Retail Distrib Manag 43(3):221–241
10. Holmes A, Byrne A, Rowley J (2012) Mobile shopping behaviour: insights into attitudes, shopping process involvement and location. Int J Retail Distribution Manage 42
11. Shankar V, Venkatesh A, Hofacker C, Naik P (2010, May) Mobile shopper marketing: key issues, current insights, and future research avenues. J Interactive Marketing 24(2):111–120
12. Maamar Z, Yahyaoui H, Mansoor W, Heuvel W (2001) Software agents and wireless E commerce. ACM SIGecom Exchanges 2(3)
13. Hui T (2011, December) Research on security framework for mobile commerce. SciVerse Science Direct Energy Procedia 13:8602–8608
14. Azfar A, Choo KR, Liu L (2016) Android mobile VoIP apps: a survey and examination of their security and privacy. Electron Commer Res 16(73)
15. Liu Y, Liu Z (2012) Android development and mobile E-commerce research. Applied Mechanics and Materials Online, vol 155–156. Trans Tech Publications, Switzerland
16. Chen X, Zhang J, Shao Q (2011, October) Application research on the mobile agent security. SciVerse ScienceDirect, Energy Procedia 11:4030–4033
17. Hao F, Geyong M, Chen J, Wang F, Lin M, Luo C, Yang L (2014) An optimized computational model for multi-community-cloud social collaboration. IEEE 7(3):346–358
18. Ta VT, Antignac T (2015) Privacy by design: on the conformance between protocols and architectures. *INRIA*. University of Lyon, France
19. Sharma H (2010) An evaluation of consumer privacy protection in E-commerce websites: a comparative study of six E-stores: part 1. The EDP Audit, Control, and Security Newsletter 42(2):1–19
20. Giannakis A, Batten L (2011, August 31) E-commerce: protecting purchaser privacy to enforce Trust, Springer Science and Business Media. Electron Commer Res 11:421–456
21. Zhang H, Li P, Zhou Z, Wu J, Yu X (2014, May) A privacy-aware virtual machine migration framework on hybrid clouds. Journal of Networks 9(5)
22. Halaweh, M. (2014). Users' perception of security for mobile communication technology, American University of the Middle East, Kuwait City,Kuwait. IGI Global
23. Lieshout MV, Kool L, Schoonhoven VB, Jonge DM (2011) Privacy by design: an alternative to existing practice in safeguarding privacy. Info 13(6):55–68
24. Chong AYL, Chan FTS, Ooi KB (2012) Predicting consumer decisions to adopt mobile commerce: cross country empirical examination between China and Malaysia. Decis Support Syst 53(1):34–43
25. Hong-yun X Research and Design of WAP-based Mobile E-Commerce System. Key Engineering Materials Volumes:474–476 (403–407)
26. Leu F, Lin C, Castiglione A (2011) Special issue on cloud, wireless and e-commerce security. Online Springer, Verlag
27. Wang Y, Wang R, Dexun X (2014) Mobile e-commerce personalized information recommendation model, Applied Mechanics and Materials. Trans Tech Publications, Switzerland
28. Kushwaha, S., Kumar, S., & Gupta, N. (September 2011). An object oriented record management system (OORMS) for M-commerce system based on J2ME wireless tool kit, Int J Adv Comput Res, 1(1), 2277–7970
29. Razaque R, Rizvi S (2017) Privacy preserving model: a new scheme for auditing cloud stakeholders. J Cloud Comput: Advances, Syst Appl. DOI:10.1186/s13677-017-0076-1
30. Rubinstein, I. (2011). Regulating privacy by design, Berkeley Technology Law Journal, 26 (3), 1409–1456
31. Pedraza, J., Patricio, A. M., Deasi, A., & Molina, J.M. (2012). Privacy-by-design rules in face recognition system. Neurocomputing
32. Kroener I, Wright D (2014) A strategy for operationalizing privacy by design. Inf Soc 30:355–365
33. D'Acquisto DG, Ferrer DJ, Kikiras P, Torra V, Montjoye Y-A, Bourka A (2015) Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. ENISA
34. Cavoukian A (2009) Privacy by design: the 7 foundational principles. Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner Ontario, Canada
35. Charith P, McCormick C, Bandara KA, Price AB, Nuseibeh B (2016, November) Privacy-by-design framework for assessing internet of things applications and platforms. The 6th International Conference on the Internet of Things (IoT 2016)
36. Jain, A.K & Shanbhag, D. (2012, October). Addressing security and privacy risks in mobile applications. IT Pro, IEEE Computer Society
37. Davies, N., & Langheinrich, M. (2013). Privacy by design. Pervasive computing *IEEE CS*, 1536–1268
38. Balboni P, Macenaite M (2013) Privacy by design and anonymisation techniques in action: case study of Ma3tch technology. Computer law & security review 29(4):330–340
39. Koops, J.B., & Hoepman, H.J., & Leenes, R. (2013). Open-source intelligence and privacy by design, Computer Law & Security Review: The International Journal of Technology Law and Practice, 29(6), 676–688
40. Li J, Liu Z, Chen X, Xhafia F, Tan X, Wong SD (2015) L-EncDB: a lightweight framework for privacy-preserving data queries in cloud computing. Elsevier Knowl-Based Syst 79:18–26
41. Yang K (2012) Consumer technology traits in determining mobile shopping adoption: an application of the extended theory of planned behavior. J Retail Consum Serv 19:484–491
42. Zhang R, Chen QJ, Lee C (2013) Mobile commerce and consumer privacy concerns. J Comput Inf Syst 53(4):31–38
43. Wu Y, Ko R, Al-Dubai A (2014) Special issue on advances in trust, security and privacy for wireless and mobile networks. Wirel Pers Commun 75(3):1587–1589
44. Alharbi MI, Zyngier S, Hodkinson C (2013) Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. J Enterp Inf Manag 26(6):702–718
45. Yang, K., Zhang K., Ren, J & Shen, X. (2015, August). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. Security and Privacy in Emerging Networks. IEEE Communications Magazine
46. Nguessan D, Martini JSC (2015, August) Framework for security and privacy Management for Mobile Middleware Based on tuple. IEEE Lat Am Trans 13(8)
47. Zhao J, Zhang W, Yuan C (2012) Research on mobile agent security of application software in open platform. Adv Mater Res 403-408:1332–1336
48. Duncan G (2007, August 31) Privacy by design. Science New Series 31(5842):1178–1179

49. Kambourakis G, Martıinez G, Marmol GF (2015) Special issue on advances in security and privacy for future mobile communications. Springer Science and Business Media, USA: New York
50. Earley S (2014) Mobile commerce: a broader perspective. IEEE 16(3):61–65
51. Leavitt, N. (2010, December). Payment Applications Make E-Commerce Mobile. IEEE Computer Society
52. Mohbey K, Thakur GS (2015) Interesting user behaviour prediction in mobile ecommerce environment using constraints. IETE Tech Rev 32(1)
53. eMarketer. (2016, May 4). Mcommerce's Rapid Growth is Primarily Coming from smartphones. Retrieved from: http://www.emarketer.com/Article/Mcommerces-Rapid-Growth-Primarily-Coming-Smartphones/1013909.
54. Davis F (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 13(3):319–339
55. Davis F, Bagozzi R, Warshaw P (1989) User acceptance of computer technology: a comparison of two theoretical models. Manag Sci 35(8):982–1002
56. Venkatesh V, Davis FD (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag Sci 46(2):186–204
57. Bhatti T (2007) Exploring factors influencing the adoption of mobile commerce. J Internet Banking and Commerce 12(3) Retrieved from: http://www.icommercecentral.com/open-access/exploring-factors-influencing-the-adoption-of-mobile-commerce.php?aid=38513
58. Ajzen I (1991) The theory of planned behaviour. Organizational Behav and Human Decision Process 50(2):179–211
59. Li C (2013) The revised technology acceptance model and the impact of individual differences in assessing internet banking use in Taiwan. Int J Bus and Inf 8(1):96–119
60. Techopedia. *Community Clouds*. Retrieved from: https://www.techopedia.com/definition/26559/community-cloud
61. Modi, K. & Jadeja, Y. (2012). Cloud Computing -Concepts, Architecture and Challenges, proceedings in 2012 international conference on computing, electronics and electrical technologies [ICCEET, 2012], 877–880
62. Rodrigues M, Gonçalves EG, Kelner J, Sadok HD, Curescu C (2016) High availability in clouds: systematic review and research challenges. Journal of Cloud Computing Advances, Systems and Applications 5(16). DOI:10.1186/s13677-016-0066-8
63. Balfanz D, Durfee G, Smetters DK, Grinter RE (2004) In search of usable security: five lessons from the field. *IEEE Security & Privacy* 2(5):19–24 See also: http://www.parc.com/work/competencies.html
64. Casalo VL, Flavian C, Miguel Guinaliu M (2007) The role of security, privacy, usability and reputation in the development of online banking. Online Inf Rev 31(5):583–603
65. Ouedraogo M, Mignon S, Cholez H, Furnell S, Dubois E (2015) Security transparency: the next frontier for security research in the cloud. J Cloud Comput Adv, Syst and Appl 4(12). DOI:10.1186/s13677-015-0037-5
66. Vanderhoof R (2003) Privacy by design. Card Technology 8(8):18–20
67. Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between providers and users of marketing research: the dynamics of trust within and between organizations, J Mark Res, 29 (August), 314–329
68. Achrol R (1991) Evolution of marketing organization: new forms of turbulent environments. J Mark 55(4):77–93
69. Dwyer FR, Schurr HP, Oh S (1987) Developing buyer-seller relationships. J Mark 51(April):11–27
70. Morgan MR, Hunt DS (1994) The commitment-trust theory of relationship marketing. J Mark 58(3):20–38
71. Parasuraman A, Berry LL, Zeithaml AV (1991) Understanding customer expectations of service. Sloan Manag Rev 32(3):39–48
72. Milnes, H. (2016, January 5). Where mobile commerce is going in 2016. Digiday. Retrieved from: http://digiday.com/brands/mobile-commerce-going-2016/
73. Hoel T, Chen W (2016) Privacy-driven design of learning analytics applications exploring the design space of solutions for data sharing and interoperability. J Learning Analytics 3(1)
74. Monreale A, Rinzivillo S, Pratesi F, Giannotti F, Pedreschi D (2014) Privacy-by-design in big data analytics and social mining. EPJ Data Science 3(1):1–26

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com