symmetry

MDPI

Article

The Effects of Applying Privacy by Design to Preserve Privacy and Personal Data Protection in Mobile Cloud Computing: An Exploratory Study

Hussain Mutlaq Alnajrani [1,2] and Azah Anir Norman [1,*]

[1] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia; hussain@siswa.um.edu.my
[2] Faculty of Computer Science and Information Technology, Albaha University, Albaha, Saudi Arabia
* Correspondence: azahnorman@um.edu.my

Received: 4 November 2020; Accepted: 6 December 2020; Published: 9 December 2020

Abstract: Mobile cloud computing (MCC) is a domain that stemmed from advances in mobile technology and cloud computing. Although debate continues about the best strategies to preserve privacy and personal data protection in MCC, it is essential to explore the effects of applying privacy by design (PbD) to preserve privacy and personal data protection in MCC. PbD is a general philosophy that demonstrates privacy should not be overviewed as an afterthought, but rather as a first-class requirement in the design of IT systems. This study explores the effects of applying PbD to preserve privacy and personal data protection in MCC, and is focused on the privacy of personal data. In this exploration, a framework using PbD has been demonstrated, and seven hypotheses were formulated. Moreover, a survey was implemented where 386 responses were used to test the formulated hypotheses. The results of this study supported the perceived benefits, cues to action of PbD, and perceived threat are positively and directly related to privacy and personal data protection behavior in MCC. Moreover, the results supported that the perceived barriers are negatively and directly related to privacy and personal data protection behavior in MCC. Overall, the results support the utilization of PbD to preserve privacy and personal data protection in MCC and encourage the practitioners to utilize PbD to preserve privacy and personal data protection in MCC.

Keywords: mobile cloud computing; privacy; personal data protection; privacy by design

1. Introduction

Today, the resources provided by mobile devices are among the most widely used media for saving and manipulating data in the current era [1,2]. However, the resources provided by mobile devices are considered to be limited. Therefore, recent developments in mobile devices have heightened the need to look for more spaces to save sensitive data and information. As a result, mobile users have utilized an available internet facility called cloud computing to keep their data. Hence, this situation leads to a new domain known as mobile cloud computing (MCC) [1].

Recently, there is an increasing demand for security, due to data breach cases worldwide [1]. For example, an organization faces a fine for the theft of data from its website in 2019 [3]. More importantly, it has been reported that people's personal data is just that personal; when an organization fails to protect it from loss, damage or theft, it is more than an inconvenience [3]. Another concern is when a firm's digitalization practices are deemed improper distribution and use of customer data [4]. Moreover, bankruptcy happened, due to a data breach [4,5].

More recently, the privacy and protection of MCC data are increasingly recognized as one of the key data issues [6,7]. For instance, in big data, research reported that relying on the number

of downloads of mobile device applications, the volume of big data has a negative effect on firm performance [4]. Additionally, a recent investigation in big data reported that it would be necessary to monitor the evolution of the issues related to legal implications associated with terms of privacy and ownership of data [8]

In spite of the seemingly convenient nature of MCC, it demonstrates various challenges for users concerning the privacy and security of their information [2]. The research reported four categories of privacy: Privacy of the person, privacy of personal data, privacy of personal behavior, and privacy of personal communication [9]. This study is focused on the privacy of personal data that refers to data protection issues [9].

Moreover, recent attention towards privacy issues by many stakeholders, including users, policymakers and companies and which are demonstrating risks for them, includes but not limited to the data breach, blackmailing, social engineering, and collection of private information [10]. Furthermore, in an attempt to address the privacy issues, for example, in Europe, laws and regulations of data exposure and location transparency is demonstrated through the general data protection regulation (GDPR) [11–13].

More recent attention has focused on providing privacy by design (PbD) to ensure that any activities conducted on an individual's data are accompanied by the provision of privacy and security of the data [14]. PbD is a procedure recommended to be followed by companies, such as cloud computing services providers. Respectfully, the study presented in this paper aims to explore the effects of applying PbD to preserve privacy and personal data protection in MCC.

In this exploration, a framework using PbD has been demonstrated adopting the health belief model (HBM) to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. The HBM is used to explore the perceived benefits, perceived barriers, perceived severity, perceived susceptibility, cues to action, and perceived threat [15–18]. Moreover, a survey has been implemented where a questionnaire has been circulated, and a pilot study has been applied with 100 responses. Furthermore, a total of 386 responses were used for the current analysis. Moreover, the SmartPLS 3.2.8 [15–21] has been utilized for the data analysis. The SmartPLS 3.2.8 is a well-known tool for statistical analysis and extensively employed in the research domain [19,20].

This study's results supported that the perceived benefits, cues to action of PbD, and the perceived threat are positively and directly related to privacy and personal data protection behavior in MCC. The results also supported that the perceived barriers are negatively and directly related to privacy and personal data protection behavior in MCC.

Generally, this study has three contributions, including introducing a new framework using PbD to preserve privacy and personal data protection in MCC. This study also adopted the HBM to explore preserve privacy and personal data protection in MCC and Evaluated applying PbD in preserving privacy and personal data protection in MCC. Overall, this study's results will help researchers and practitioners, including managers and policymakers, with the necessary perception when utilizing PbD to preserve privacy and personal data protection in MCC.

The remainder of this paper is structured as follows. Section 2 presents the research background and motivation. Section 3 describes the exploratory study. Section 4 shows the results and discussion. Section 5 clarifies the threat to validity. Section 6 presents a comparison with related work. Finally, Section 7 demonstrates the conclusion.

2. Background and Motivation

This section presents a general background of MCC, PbD, and the need for an exploratory study.

2.1. Mobile Cloud Computing

Today, the resources provided by mobile devices are among the most widely used media for saving and manipulating data. In general, the resources provided by mobile devices are considered to be limited, such as memory size, disk capacity, and computational resources [22]. Currently, mobile users

have utilized an available internet facility called cloud computing to save their data [22,23]. Hence, this situation leads to a new domain known as MCC [24]. As shown in Figure 1, the MCC user utilized cloud service for processing and storing personal data.

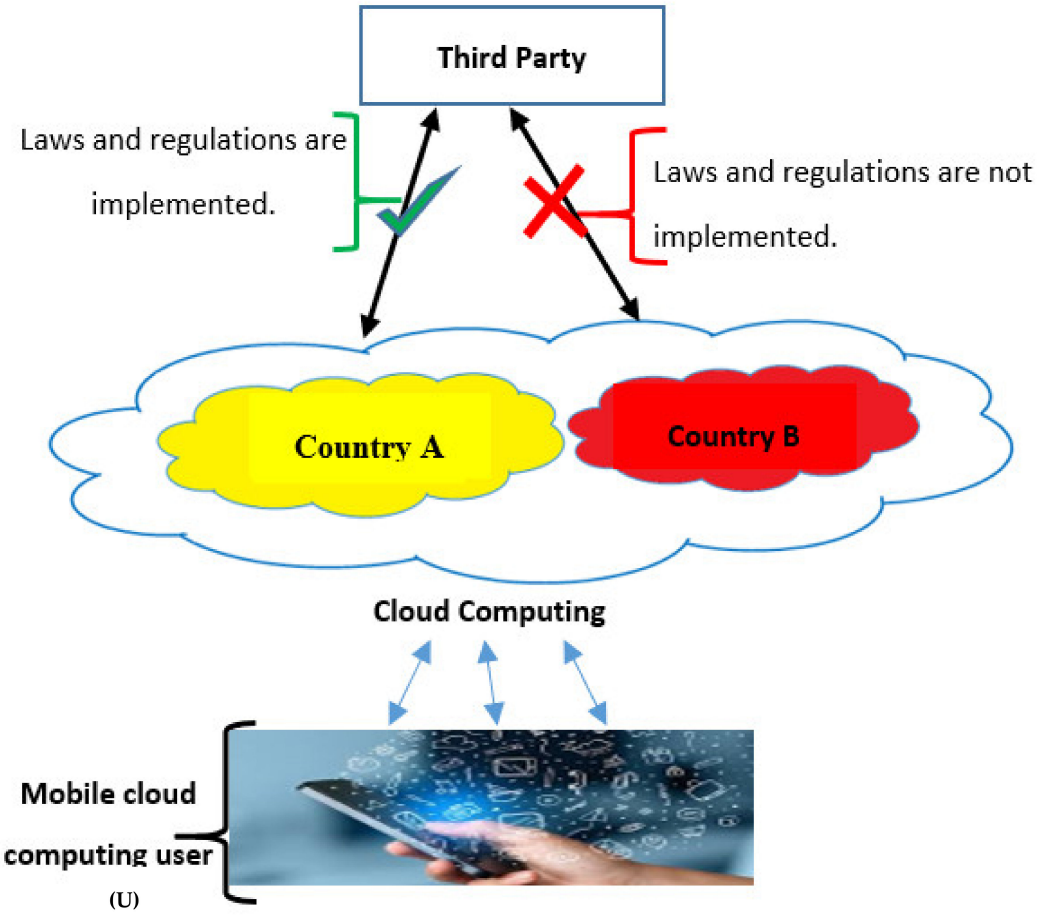


Figure 1. A systemic diagram of personal data in MCC.

As shown in Figure 1, a scenario of privacy in MCC is illustrated. An MCC user (U) has the demand to utilize the cloud service to process and store his personal data that require privacy. In the same case, the cloud service is located in different countries, for instance, country (A) and country (B). Country (A) that hosted the cloud service provider is applied GDPR, or it is equivalent laws and regulations. On the other hand, Country (B) hosted the cloud service provider does not apply GDPR or equivalent laws and regulations.

The research reported that the cloud service located in a country that does not apply laws and regulations regarding privacy and personal data protection in MCC is subject to privacy violation (data exposure, misuse) by a third-party [25–29]. In turn, the main issue demonstrated in Figure 1 is the processing of the user's personal data (U) in the country (B) hosted the cloud service provider and did not apply GDPR, or it is equivalent laws and regulations.

It interesting to note that MCC preserves the mobile resource, including the data and applications on external providers to the mobile device [24]. For example, it can store personal data, private family information, and private personal life stories. In general, the user can access the data regardless of his current location. MCC is a domain that has resulted from advances in mobile technology and cloud computing [24].

As demonstrated in Figure 2, MCC's architecture offers a model combining the benefits of both mobile technology and cloud computing. The figure shows that the corresponding mobile users can

utilize mobile devices, such as tablets, PDAs, and smartphones attached to the networks via the base transceiver station (BTS) or satellite.

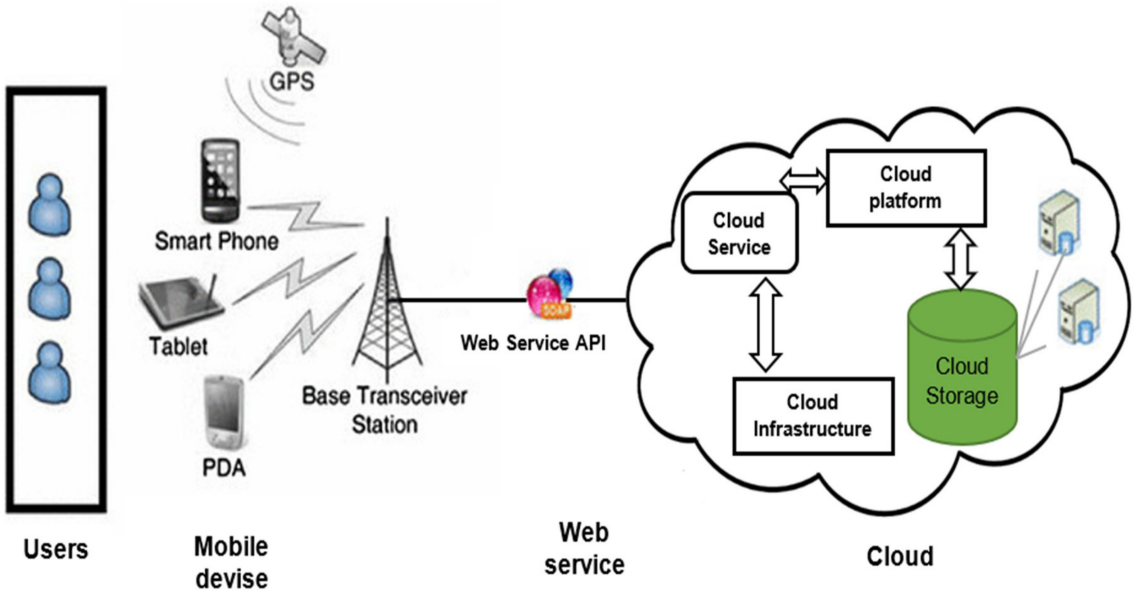


Figure 2. Architecture of MCC [30].

As presented in Figure 2, mobile users' requirements are broadcasted to the servers that offer mobile services, then, the subscribers' requests are distributed to the cloud service using the Internet, and finally, the controllers in the cloud send the users the requested medical cloud services.

2.2. Privacy by Design

Several studies investigating personal have shown that personal data is associated with the collection, use, disclosure, storage, and destruction of personal data (or personally identifiable information, PII). Previous research has reported that the identification of private information depends on the specific application scenario, law and regulation is the key task of personal data protection [31].

More recent attention has focused on providing PbD to ensure that any activities conducted on an individual's data are accompanied by the provision of privacy and security of the data [14]. PbD is a procedure recommended to be followed by cloud computing services providers [32].

Previous research has indicated that PbD is founded upon seven key principles, as defined by Cavoukian [14]. The principles are proactive, not Reactive, preventive, not Remedial, privacy by default, privacy embedded into the design, privacy by positive-sum, not zero-sum, an end-to-end security-full life cycle protection, visibility, and transparency, and finally, respect for user privacy [14,33]. For this study, we focus on visibility and transparency represented by location transparency. The location transparency will help the MCC users to choose the country that applies laws and regulations for cloud storage to protect their data.

2.3. The Need for an Exploratory Study

Several researchers have determined using cloud computing for saving mobile data [1]. As a result, privacy and personal data protection in MCC are currently one of the main hurdles in privacy defense issues [12]. For example, an investigation state that data on the cloud might be stored at multiple locations across different states and countries that might be secure in one country and may not be protected in another [34]. Besides, the nature of cloud computing has important implications for the privacy of personal information, including questions about how secure the location is and who has access to it [34,35], which affects the MCC user's decision to use cloud storage [35].

Moreover, questions have been raised about threats and attacks of personal data privacy; research reported that improper security policies and practices in some locations are one of the issues of privacy and personal data protection in MCC [2,34,36,37]. However, the issue of privacy and personal data protection in MCC may cause laws and regulations noncompliance and also threats and attacks, such as leakage of user privacy, data misuse, disclosing information or data, and identity theft [2], and may even jeopardize personal data privacy where the MCC users might be exposed to, for instance, a spy, steal the user information, spam messages, social trolling and shaming, and internet viruses [38,39]. Appendix B displays examples of privacy issues presented in the literature.

Although the debate continues about the best strategies for dealing with the various issues for privacy and personal data protection in MCC, the benefits of utilizing PbD for privacy and personal data protection in MCC are not explored. Specifically, no single study exists which explored the effects of applying PbD for privacy and personal data protection in MCC [2,40]. PbD is a general philosophy that demonstrates privacy should not be overviewed as an afterthought, but rather as a first-class requirement in the design of IT systems [41]. Consequently, this study aims to explore the effects of applying PbD to preserve privacy and personal data protection in MCC.

3. Exploratory Study

This section presents our exploratory study in four subsections. Section 3.1 highlights the purpose of this study. Section 3.2 presents a proposed framework. Section 3.3 illuminates the research model. Section 3.4 demonstrates the development of the survey instrument and data collection and analyses.

3.1. Purpose of the Study

This research aims to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. Table 1 shows the research questions (RQs) and research objectives (Ros) of this study.

Table 1. Research questions and research objectives of this study.

#	Research Question	Research Objective
1	How to preserve privacy and personal data protection in mobile cloud computing using privacy by design framework?	To illustrate applying privacy by design framework to preserve privacy and personal data protection in MCC.
2	How does the privacy by design framework effects preserving privacy and personal data protection in MCC?	To evaluate the privacy by design framework in preserving privacy and personal data protection in MCC.

In the following Subsections, Section 3.2 demonstrates our proposed framework to answer RQ 1, and Subsection C illustrates our research model to replay RQ 2.

3.2. Proposed Framework

Notably, MCC is the combination of cloud computing and mobile computing to bring rich computational resources to mobile users, network operators, as well as cloud computing service providers [42]. Currently, MCC provides business opportunities for mobile network operators, as well as cloud providers [43]. Conspicuously, research defined MCC as "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle" [42].

This study proposes the utilization of PbD to preserve privacy and personal data protection in MCC using visibility and transparency, considering location transparency, laws, and regulations.

To help with selecting the cloud storage, which hosted in countries applied laws and regulations for privacy and personal data protection in MCC.

This study proposed to include allowing the MCC user to select a storage location, including the country, cloud storage, and laws and regulations applied. By doing this, visibility of location transparency and laws and regulations were considered to be implemented. As shown in Figure 3, the proposed framework has two phases, including registration and synchronization. The proposed framework phases are highlighted as follows:

A. Registration phase: In this phase, the MCC user must register for using the MCC storage service. In addition to providing the basic data, the MCC user must select the storage location classified based on applying laws and regulations in the MCC storage service locations.

B. Synchronization phase: In this phase, the MCC storage service provides synchronization in the existing storage services [44]. In synchronization, personal data on a mobile device are synced to a server that leads to an MCC storage service location. The added, modified, or deleted data will automatically reflect in the selected storage location using upload and download processes [45]. The proposed framework utilizes the existing synchronization process, adding the location, including the ability to know the location of the storage that the user is synchronized with.

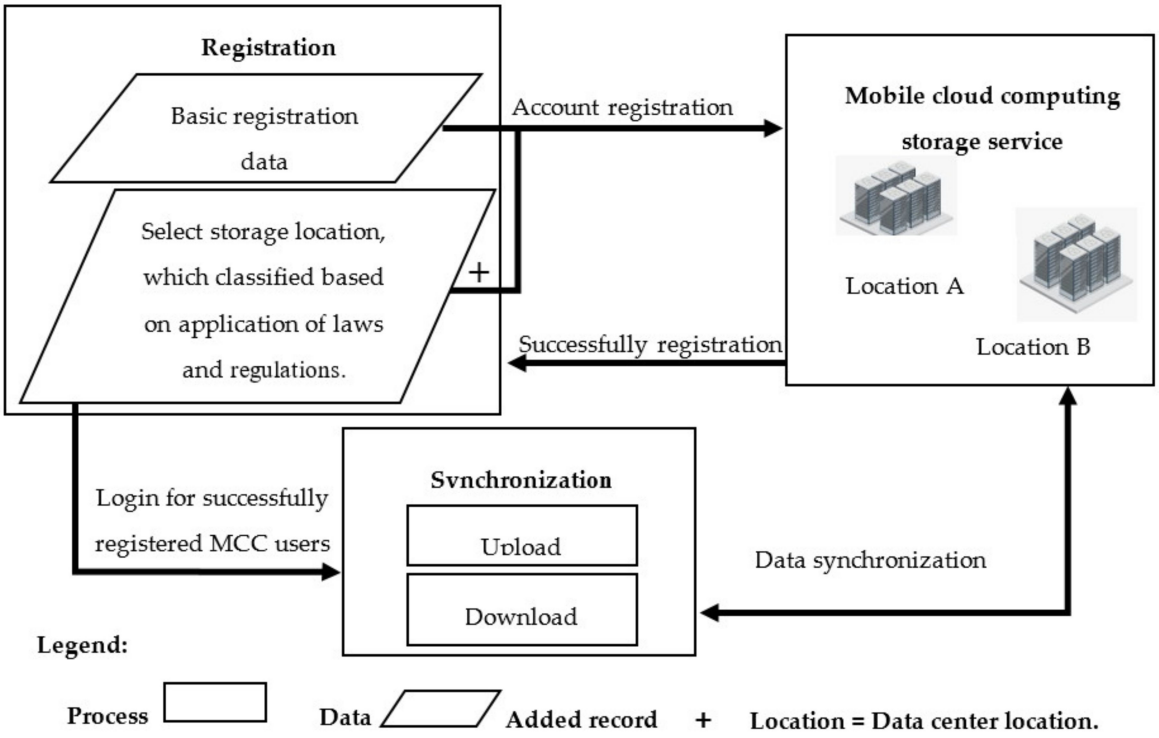


Figure 3. The high-level architecture of the proposed framework.

3.3. Research Model

For this research, the objective of the study presented in this paper is to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. For this exploration, we have borrowed the HBM [46,47] to explore the effects of applying PbD to preserve privacy and personal data protection in MCC.

The HBM is a conceptual framework currently utilized in empirical preventive health care studies by asking respondents what behaviors they engage in particular issues [46,47]. Appendix A shows the health belief model.

In general, the HBM is utilized in the research domain to highlight how programs need to consider individual beliefs in the issue being addressed. Furthermore, the HBM is useful for measuring

behavioral intention or likelihood of behavior as the dependent variable [15]. Moreover, the HBM is helpful in recognizing violations and threats in the examination issues [48].

Generally, the HBM was utilized in information systems' security domain [15,19,20,49–51]. In addition, the current study adopts the HBM for the following reasons:

- The HBM tackles personal human issues towards assessing and modeling the impacts of the diseases [15,19,20,49–51]. Information systems security experts have adopted the HBM for modeling and assessing personal issues, such as personal data protection and privacy. Obviously, there are many privacy and personal data protection factors that have causes and impacts, which can be assessed by the HBM.
- The HBM can enrich the PbD in MCC through providing cues to action (refers to experiences and applying location transparency for MCC storage location), where cues to action is distinguishing the HBM from other theories, such as Technology Acceptance Model (TAM) [52], Theory of Reasoned Action (TRA) [53], and Theory of Planned Behavior (TPB) [54].
- The HBM can be used to measure the effects of applying PbD to preserve privacy and personal data protection in MCC, since the perceived threat and its underlying relationship to privacy and personal data protection behavior for MCC can be investigated by the HBM.

For this exploration, to assess the proposed solution, the HBM is utilized for evaluating preserve privacy and personal data protection in MCC by questioning the users regarding the perceived benefits, perceived barriers, cues to action, and perceived threat when the visibility of location transparency, laws, and regulations are implemented.

As shown in Figure 4, the HBM is demonstrated in a conceptual framework that utilized the predictive value of the original constructs of the HBM. Figure 4 shows the predictive value of the HBM original constructs, including the perceived benefits, perceived barriers, Cues to Action of PbD, and perceived threat, which combined perceived severity and perceived susceptibility [15–18].

In this study, Privacy and data protection behavior in MCC refer to the actions of a country that hosted the actual cloud storage and their behaviors against malicious behavior and violation regarding MCC. Perceived benefits refer to altering a person's behavior if there will be some perceived benefits in adopting new behavior [18]. In this context, it indicates the perceived effectiveness of location transparency of cloud storage. The following hypothesis is formulated:

Hypothesis 1 (H1). *Perceived benefits are positively related to privacy and personal data protection behavior in MCC.*

Perceived barriers could act as restrictions considering a person acting according to recommended behavior. Even though a person might feel that a certain action is powerful in reducing the threat, the action in question might cause him unnecessary pain or other inconvenience [55]. In this context, MCC users perceived the unavailability of location transparency and unsatisfactory data protection laws and regulation. The following hypothesis is formulated:

Hypothesis 2 (H2). *Perceived barriers are negatively related to privacy and personal data protection behavior in MCC.*

Cues to action of PbD in the HBM are occurrences that encourage people to alter their behavior [16]. As confirmed in Dodel et al. and Vatka [55,56], if a person has previously been afflicted, he might detect upcoming concerns easier [55,56]. The cues to action in this study pointing directly to the perceived threat, and also directly to privacy and personal data protection behavior in MCC to demonstrate if the cues to action have an impact on individual threat perception. The following hypotheses are formulated:

Hypothesis 3 (H3). *Cues to action of PbD considering visibility location transparency, laws, and regulations are positively related to the perceived threat.*

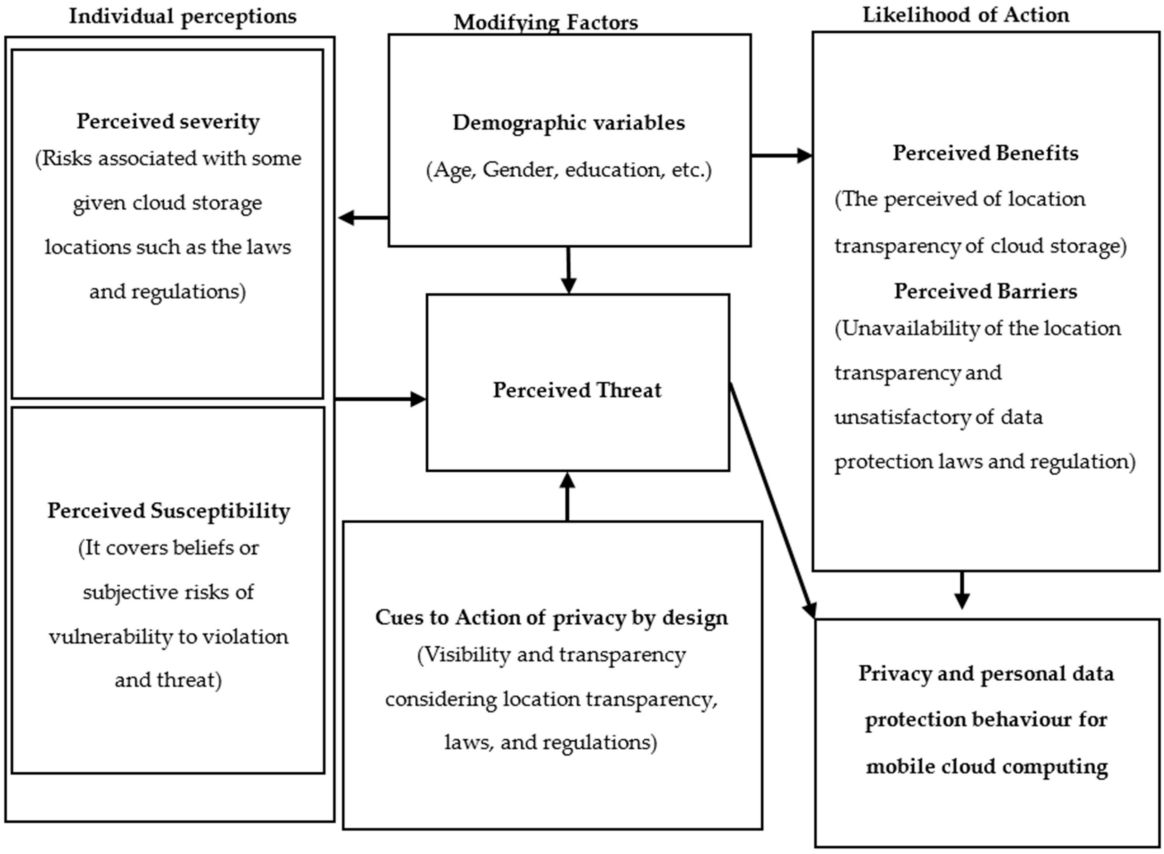


Figure 4. A conceptual framework based on the health belief model (HBM).

Hypothesis 4 (H4). *Cues to action of PbD considering visibility location transparency, laws, and regulations are positively related to privacy and personal data protection behavior in MCC.*

Perceived threat, in the HBM, the perceived threat is affecting the individual's intent to implement health-related behavior [16]. According to Edwards and Glanze et al. [16,57], the perceived threat is a combination of perceived severity and perceived susceptibility to the disease or condition. The following hypothesis is formulated:

Hypothesis 5 (H5). *The perceived threat is positively related to privacy and personal data protection behavior in MCC.*

Perceived severity is related to a person's perception of how serious a health problem is [55]. In this study, the perceived severity or seriousness is related to risks associated with some given cloud storage locations, such as the laws and regulations related to privacy and personal data protection in MCC. The following hypothesis is formulated:

Hypothesis 6 (H6). *Perceived severity is positively related to privacy and personal data protection behavior in MCC through perceived threat.*

Perceived susceptibility covers beliefs or subjective risks of disease progression. The person may be more cautious, and therefore, feel threatened by the disease. On the other hand, the person may deny the possibility of contracting the disease—although both are provided with the same information and facts about the disease [15]. In this study, if an MCC user sees the outstanding vulnerability to violation and threat, one is more likely to take further countermeasures according to their privacy and data protection behavior in MCC. The following hypothesis is formulated:

Hypothesis 7 (H7). *Perceived susceptibility is positively related to privacy and personal data protection behavior in MCC through perceived threat.*

As shown in Figure 5, the integration of formulated hypotheses has six constructs based on the HBM [18]. Moreover, in this study, the second-order construct is utilized to measure the perceived threat modeled as a second-order formative construct [58]. The perceived threat includes perceived severity and perceived susceptibility as two underlying dimensions [57]. The perceived threat is suitably modeled as a second-order formative construct following Williams et al. [20] recommendation. The constructs defined and their related hypotheses are as follows:

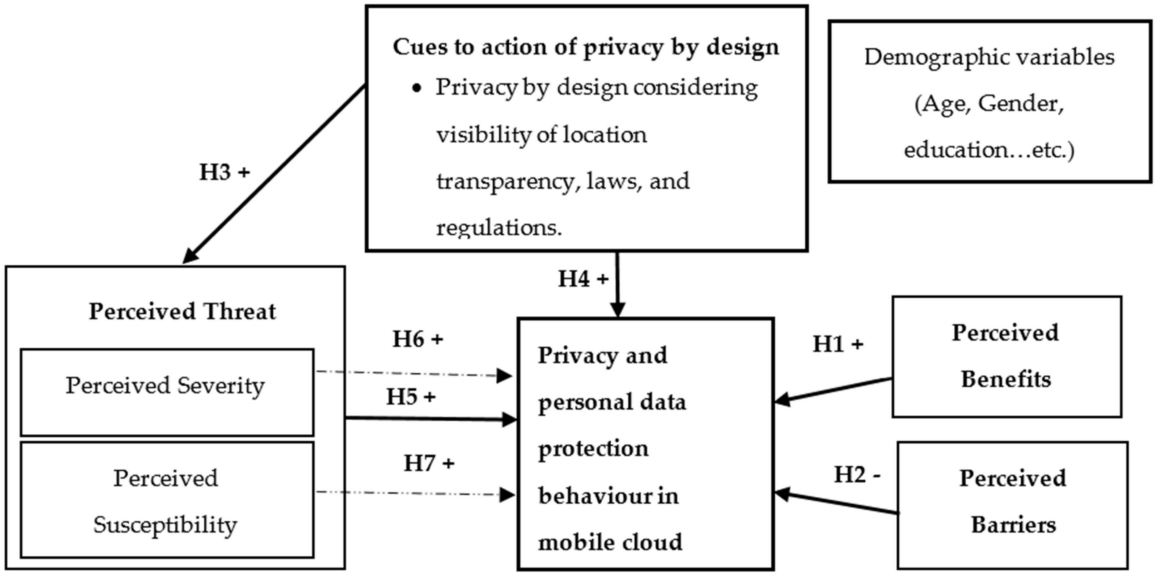


Figure 5. Integration of formulated hypotheses based on the HBM.

3.4. Development of Survey Instrument, and Data Collection and Analyses

For this analysis, the instruments, validity, and reliability of this investigation, and data collection and analysis were implemented as follows:

3.4.1. Instruments

In this study, the questionnaire is divided into two parts, as follows:

1. The first part consists of the demographical data of the respondents, such as Age, Gender, Marital status, Level of education, and Cloud storage.
2. The second part contains the constructs, which were ordered as follows:

- **Perceived threat:** It contains two sub-dimensions, including the perceived susceptibility to violation and threat and perceived severity of risks associated with some given cloud storage locations that do not apply laws and regulations for privacy and personal data protection in MCC. In summary, perceived susceptibility and perceived severity were measured by 4 and 5 items, respectively, adopted from the Al Khater study and self-developed [59].
- **Perceived benefits** were assessed by the six items developed by Al Khater study and self-developed [59].
- **Perceived barriers** were assessed by the four items developed by Al Khater study and self-developed [59].

- **Cues to Action of PbD** were assessed by the six items developed by Al Khater study and self-developed [59].
- **Privacy and data protection behavior in MCC** are assessed by the five items developed by Al Khater study and self-developed [59].

For all of the defined constructs, the measurement was followed is the 5-point Likert-type scale [60], including 1 = strongly, agree, 2 = agree, 3 = undecided, 4 = disagree, and 5 = strongly disagree.

3.4.2. Validity and Reliability

For this research, the objective of the study presented in this paper is to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. In this study, a questionnaire is implemented through a web-based survey tool named Google forms [61]. To ensure validity and reliability, the questionnaire was sent to experts in the domain to test the validity [62,63]. To be specific, sending a questionnaire for validation to experts is consistently utilized in the research domain [64]. Accordingly, the first draft of the questionnaire was received by a panel of experts, made up of two tenure/track faculty members at the University of Malaya and one of MCC security experts to guarantee the validity of the questionnaire.

Moreover, the questionnaire was distributed to 100 respondents as a pilot study. A pilot test is considered an essential phase to identify potential problem areas and shortcomings in the research instrument [65]. Based on the results of the pilot study, the questionnaire was improved and sent again to experts to test the validity after the pilot study.

3.4.3. Data Collection and Analysis

In this study, a questionnaire was distributed with a cover letter to explain the purpose of the research via online platforms, including Facebook and LinkedIn. The purposive sampling was used [66,67] in this study; therefore, the participants comprised the users who used cloud platforms in MCC to store their data. The questionnaire link was shared with over 600 possible respondents on LinkedIn and over 550 contacts through Facebook.

As a result, a total of 386 responses were received. Since all the questions in the questionnaire are mandatory, the incomplete survey is automatically not allowed to continue; therefore, all of the sample 386 responds have completed the answers to all the questions.

As presented in Hair et al., the sample size of the main study is recommended to be 100–150 is the model contains seven or fewer constructs [68]. Moreover, the minimum sample size is recommended to be ten times the highest number of structural paths to a latent variable [69]. Furthermore, Creswell (2012) suggested that the minimum sample size is 350 responses for a survey [70]. So, the sample size of this study is 386, which is considered to be sufficient [68–70].

It is interesting to note that a study reported comparisons of response rates for online surveys and paper-based surveys, the results revealed that in paper-based surveys, the overall response rate is amounting to 56% [71]. On the other hand, the overall response rate for online surveys is 33% [71]. Moreover, research points out that online surveys' response rate is 30%, on average [72]. For this study, the response rate is equal to 33.56%, which is considered average [71,72]. Simply, for this study, the response rate is the number of responses (386) divided by the number of people we invited to respond (1150) multiply by 100 [71,72].

As shown in Table 2, 195 of 386 respondents (50.52%) were in the 30 to 39 age group, 306 of 386 participants (79.27%) were a male in gender group, 234 of 386 (60.62%) were married, 192 of 386 (49.74%) reported that they had a Bachelor's degree, and 177 of 386 participants (45.85%) reported that they used Google Drive as cloud storage.

For this research, the objective of the study presented in this paper is to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. In this study, Partial Least Squares (PLS) in SmartPLS 3.2.8 [21] was used to analyze the collected data. In particular, PLS is well

appropriate to expound complex relationships by averting unacceptable solutions problems and not identifying factors [73].

Table 2. Descriptive statistics of demographic characteristics of participants.

Demographic	Category	Percentage	Number of Participate
Age	19 or younger	0.78%	3
	20 to 29	29.53%	114
	30 to 39	50.52%	195
	40 or older	19.17%	74
Gender	Male	79.27%	306
	Female	20.73%	80
Marital status	Single	34.97%	135
	Married	60.62%	234
	Divorced	4.40%	17
Education level	Elementary/Primary education	0.52%	2
	High school diploma	3.63%	14
	Bachelor's degree	49.74%	192
	Master's degree	39.38%	152
	Ph.D./Doctorate	6.74%	26
Cloud storage	Google Drive	45.85%	177
	Dropbox	16.32%	63
	One Drive (formerly Sky Drive)	8.03%	31
	iCloud	21.24%	82
	Others	8.55%	33

The data was transferred to SmartPLS software by uploading the Comma Separated Values File (.csv). The data was transferred through intermediary software (Microsoft Excel) to clean the data, which transmits the original data documents to a computer database. The excel sheet file was saved as a Comma Separated Values File (.csv) to allow the SmartPLS software to read the file.

In general, the SmartPLS is utilized to generate two main models [64] as follows.

A. Measurement model:

The measurement model comprises relationships among the latent variables and their indicators (items) [20]. In SmartPLS, to measure the items loading, to check the significance of each question, within each construct in the form of t-values, bootstrapping can be found under the calculate list [64,74]. Moreover, convergent validity, reliability, and discriminant validity [20] are measured using the SmartPLS [20,73,75].

According to Hair et al. [69], the convergent validity is known as the internal consistency scale; according to Fornell et al. [73], the discriminant validity is the degree to which the measures of different constructs are distinct from one another. Moreover, the variance inflation factor (VIF) is used to evaluate multicollinearity [20]. In general, convergent validity is measured by the average variance extracted (AVE) [75]. The reliability is assessed by composite reliability (CR) [75] and Cronbach's Alpha (CA) [75]. On the other hand, discriminant validity is evaluated by cross-loadings of the key measurement items in the model [75] and the Fornell-Larcker criterion [75].

B. Structural model:

The structural model is used to check out the hypothesis and in which by SmartPLS can be calculated the Coefficient of determination (R-squared) and path coefficient for each hypothesis [64].

In broad, the path coefficient includes the latent variables and T-test values [64]. R-squared (R^2) value of the endogenous variables is utilized to assess the predictive power of a specific model or construct and determining the standard path coefficient of each relevant exogenous and endogenous variable [76].

4. Results and Discussion

In this section, we present and discuss the results of this study. Section 4.1 shows the results, while Section 4.2 illustrates a discussion of the obtained results.

4.1. Results

This Subsection presents the results of this study, including the results of the measurement model, structure model.

4.1.1. Results of Measurement Model

For this research, the objective of the study presented in this paper is to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. For this study, convergent validity, reliability, and discriminant validity [20] results, as follows:

A. Convergent validity and reliability

As shown in Table 3, all scales show adequate values with an average variance extracted (AVE) exceeding 0.50, composite reliability (CR) scores exceeding 0.70, and Cronbach's Alpha (CA) scores greater than 0.70 [75]. Based on the obtained results in Table 3, we have noted that our AVE results are satisfactory according to the demonstration of Chin et al. [77], Fornell et al. [73], and Nunnally et al. [78], the AVE should be exceeding 0.5 to be at a satisfactory level [73,77,78]. The CR results in Table 3 are satisfactory based on the presentation of Chin et al. [77], Fornell et al. [73], and Nunnally et al. [78] if the CR scores exceeding 0.70 is satisfactory [73,77,78]. Moreover, the CA outcomes are acceptable according to the presentation of Hair et al. [79], the CA with the range starts from 0.713 to 0.917 is acceptable [79]. Furthermore, According to Petter et al. [80] and Williams [20], the VIF values ranged a threshold of 3.3 is recommended. For this study, the VIF values ranged from 1.293 to 2.741. Thus, the result in Table 3 provided evidence that multicollinearity is not a threat to the validity of the measures [20].

Table 3. Convergent validity.

Constructs	Items	Loading	VIF	AVE	CR	CA
Perceived Severity	P.SEV1	0.805	1.696	0.504	0.835	0.752
	P.SEV2	0.753	1.514			
	P.SEV3	0.653	1.297			
	P.SEV4	0.666	1.309			
	P.SEV5	0.661	1.293			
Perceived Susceptibility	P.SUS1	0.787	1.631	0.586	0.849	0.762
	P.SUS2	0.844	1.877			
	P.SUS3	0.711	1.351			
	P.SUS4	0.711	1.359			
Perceived Benefits	P.BEN1	0.716	1.913	0.608	0.903	0.871
	P.BEN2	0.742	1.977			
	P.BEN3	0.822	2.314			
	P.BEN4	0.834	2.466			
	P.BEN5	0.740	1.711			
	P.BEN6	0.817	2.024			
Perceived Barriers	P. BAR1	0.721	1.304	0.582	0.847	0.764
	P. BAR2	0.817	1.516			
	P. BAR3	0.792	1.696			
	P. BAR4	0.716	1.584			

Table 3. *Cont.*

Constructs	Items	Loading	VIF	AVE	CR	CA
Cues to Action of Privacy by design	CAPD1	0.699	1.561	0.597	0.898	0.864
	CAPD2	0.787	2.033			
	CAPD3	0.804	2.065			
	CAPD4	0.706	1.500			
	CAPD5	0.826	2.494			
	CAPD6	0.804	2.298			
Privacy and personal data protection behavior in MCC	PDBPMCC1	0.728	1.610	0.671	0.910	0.876
	PDBPMCC2	0.819	2.048			
	PDBPMCC3	0.868	2.557			
	PDBPMCC4	0.830	2.626			
	PDBPMCC5	0.844	2.741			

Note: Average variance extracted (AVE) 0.50. Composite reliability (CR) scores should exceed 0.70. Cronbach's Alpha (CA) scores greater than 0.70.

As presented in Table 3, the loadings of all reflective indicators exceeded the required cut-off level of 0.60, as recommended by Bagozzi et al. [81]. Moreover, the items of loading from the minimum value of 0.50 are valid, as suggested by Hair et al. [68].

B. Discriminant validity

As shown in Table 4, the cross-loadings resulted in adequate values (with yellow highlights). Hair et al. (2011) suggest that each measurement item should have higher loading on its own key construct than any other key construct [69]. In this study, cross-loadings measures show adequate discriminant validity and are satisfied as suggested in Gefen et al. [82,83] that the measures should load more on their construct than others to evaluate the discriminant validity of the reflective measures [82,83].

Table 4. Cross-loadings.

	CAPD	P. BAR	P. BEN	P.SEV	P.SUS	PDPBMCC
CAPD1	**0.699**	0.369	0.414	0.223	0.242	0.440
CAPD2	**0.787**	0.348	0.570	0.183	0.203	0.598
CAPD3	**0.804**	0.420	0.602	0.295	0.279	0.626
CAPD4	**0.706**	0.378	0.444	0.311	0.267	0.524
CAPD5	**0.826**	0.378	0.558	0.239	0.225	0.596
CAPD6	**0.804**	0.464	0.519	0.288	0.299	0.598
P.BAR1	0.357	**0.721**	0.255	0.359	0.390	0.255
P.BAR2	0.458	**0.817**	0.342	0.439	0.428	0.304
P.BAR3	0.391	**0.792**	0.258	0.562	0.567	0.249
P.BAR4	0.324	**0.716**	0.198	0.500	0.561	0.167
P.BEN1	0.558	0.350	**0.716**	0.227	0.209	0.454
P.BEN2	0.525	0.292	**0.742**	0.192	0.181	0.431
P.BEN3	0.547	0.291	**0.822**	0.173	0.178	0.536
P.BEN4	0.539	0.259	**0.834**	0.120	0.122	0.552
P.BEN5	0.497	0.185	**0.740**	0.106	0.070	0.524
P.BEN6	0.511	0.301	**0.817**	0.272	0.212	0.594
P.SEV1	0.257	0.452	0.200	**0.805**	0.511	0.220
P.SEV2	0.199	0.443	0.100	**0.753**	0.494	0.149
P.SEV3	0.167	0.348	0.129	**0.653**	0.375	0.138
P.SEV4	0.351	0.532	0.264	**0.666**	0.486	0.295
P.SEV5	0.203	0.337	0.128	**0.661**	0.418	0.180
P.SUS1	0.349	0.499	0.227	0.530	**0.787**	0.248
P.SUS2	0.220	0.493	0.127	0.538	**0.844**	0.167
P.SUS3	0.274	0.436	0.128	0.422	**0.711**	0.255
P.SUS4	0.157	0.469	0.146	0.483	**0.711**	0.104

Table 4. *Cont.*

	CAPD	P. BAR	P. BEN	P.SEV	P.SUS	PDPBMCC
PDPBMCC1	0.575	0.334	0.456	0.326	0.293	**0.728**
PDPBMCC2	0.637	0.297	0.526	0.251	0.188	**0.819**
PDPBMCC3	0.644	0.268	0.545	0.203	0.211	**0.868**
PDPBMCC4	0.563	0.226	0.558	0.192	0.168	**0.830**
PDPBMCC5	0.584	0.225	0.637	0.167	0.174	**0.844**

Note: P.BAR = Perceived Barriers; CAPD = Cue to Action of privacy by design; P.BEN = Perceived Benefits; P.SEV = Perceived Severity; P. SUS = Perceived Susceptibility; PDPBMCC = Privacy and data protection behavior in MCC.

As shown in Table 5, based on the Fornell-Larcker criterion, the discriminant validity is assessed by comparing the correlations between constructs with the square root of the AVE for the construct [73,75]. Fornell-Larcker criterion resulted in adequate values (with yellow highlights) with values of the key constructs higher on themselves than with other constructs [73,75] and that are satisfied based on Fornell and Larcker [73,75].

Table 5. Discriminant Validity (Fornell-Larcker criterion).

	CAPD	P.BAR	P.BEN	P.SEV	P.SUS	PDPBMCC
CAPD	**0.772**					
P.BAR	0.510	**0.763**				
P.BEN	0.676	0.355	**0.780**			
P.SEV	0.333	0.598	0.232	**0.710**		
P.SUS	0.328	0.620	0.206	0.647	**0.765**	
PDPBMCC	0.735	0.330	0.666	0.278	0.252	**0.819**

C. Second-order

As shown in Figure 6, the paths of the underlying perceived threat dimensions are significant (SEV: b = 0.571, $p < 0.001$; SUS: b = 0.529, $p < 0.001$). Moreover, the path weights of all individual indicators on the second-order construct are significant at $p < 0.001$, according to Wetzels et al. [58], guidelines.

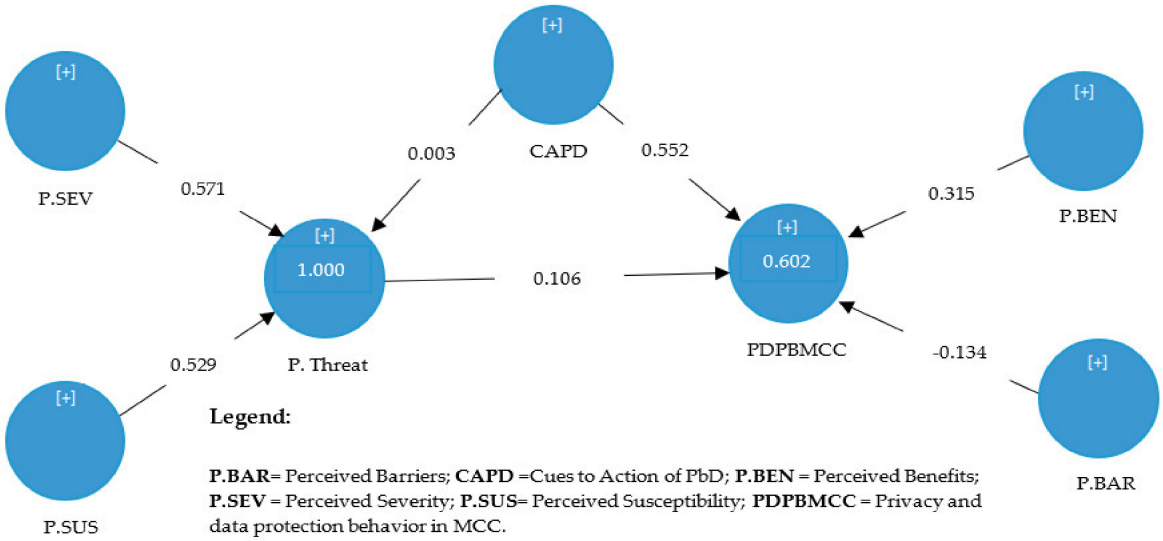


Figure 6. SmartPLS results.

4.1.2. Results of Structural Model

For this research, the objective of the study presented in this paper is to explore the effects of applying PbD to preserve privacy and personal data protection in MCC. After evaluating the

measurement model, the structural model was then analyzed. The structural model includes the assumed hypothesized relationship between exogenous and endogenous variables in the model. The results of the structural model are shown in Table 6.

Table 6. The results of the structural model.

Hypo	Relationship	Std. Beta	Std. Error	T-value	*p*-Value	R^2	Decision
H1	P. BEN → PDPBMCC	0.315	0.056	5.660	0.000		Supported **
H2	P. BAR → PDPBMCC	−0.134	0.052	2.581	0.005		Supported **
H3	CAPD → P. Threats	0.003	0.001	2.158	0.015	0.602	Supported *
H4	CAPD → PDPBMCC	0.552	0.056	9.884	0.000		Supported **
H5	P.Threats → PDPBMCC	0.106	0.043	2.438	0.007		Supported *
			Indirect Influence				
H6	P. SEV → PDPBMCC	0.060	0.025	2.435	0.007		Supported *
H7	P. SUS → PDPBMCC	0.056	0.023	2.438	0.007		Supported *

Note: Significant at * $p < 0.05$, ** $p = <0.01$.

The illustrative power of the estimated model can be evaluated by monitoring R^2 of the endogenous constructs. Chin [74] suggests that the R-squared values above 0.67 are considered high, while values ranging from 0.33 to 0.67 are moderate, whereas values from 0.19 to 0.33 are weak, and any R^2 values less than 0.19 are unacceptable. Falk et al. [84] propose an R-squared value of 0.10 as a minimum acceptable level. The value of R^2 obtained from our analysis was 0.602, indicating that 60.2% of the variance can be demonstrated by all the exogenous variables in the model.

4.2. Discussion

This Subsection illustrates a discussion of this study's results, including an analysis of the hypotheses testing.

As illustrated in Figure 6 and Table 6, the hypothesis test result of privacy and data protection behavior in MCC were analyzed using the path analysis model [85]. The results analysis and hypotheses testing are discussed as follows:

For Hypothesis 1 (H1), as illustrated in Table 6 and Figure 6, the result of this study is highly supported the perceived benefits are positively related to privacy and personal data protection behavior in MCC (b = 0.315, SE = 0.56, p = 0.000). The current result is now lead to the same findings of the previous work by Ng et al. [15], Claar et al. [49], Humaidi et al. [19,50], Williams et al. [20], and Koloseni et al. [51] that the perceived benefits are positively related to behavior [15,19,20,49–51].

For Hypothesis 2 (H2), as shown in Table 6 and Figure 6, the result of this study is highly supported perceived barriers are negatively related to privacy and personal data protection behavior in MCC (b = −0.134, SE = 0.52, p = 0.005). Indeed, the perceived barriers are negatively related as founded in previous work by Ng et al. [15], Claar et al. [49], Humaidi et al. [19,50], Williams et al. [20], and Koloseni et al. [51].

For Hypothesis 3 (H3), As illustrated in Figure 6 and Table 6, the result of this study is supported that cues to action of PbD considering visibility location transparency, laws, and regulations are positively related to the perceived threat (b = 0.003, SE = 0.001, p = 0.015). The outcome of this study is committed to the same conclusion highlighted by Edwards [16], where the cues to action are positively related to a person's perception of an event being a security threat [16].

For Hypothesis 4 (H4), as shown in Table 6 and Figure 6, the result of this study is highly supported that cues to action of PbD considering visibility location transparency, laws, and regulations are positively related to privacy and personal data protection behavior in MCC (b = 0.552, SE = 0.056, p = 0.000). Indeed, the current outcome highly supported that the location transparency with laws and regulations will help users avoid privacy violations. Furthermore, the current finding is consistent with the findings of Claar et al. [49] that cues to action is positively related to behavior [49].

For Hypothesis 5 (H5), as shown in Table 6 and Figure 6, the result of this study is supported that the perceived threat is positively related to privacy and personal data protection behavior in MCC

(b = 0.106, SE = 0.043, p = 0.007). The most exciting finding was that this examination draws the same proceeding of previous work by Edwards [16] that the perceived threat is positively related to security behavior [16].

For Hypothesis 6 (H6), as demonstrated in a group of previous studies by Ng et al. [15], Humaidi et al. [19], and Koloseni et al. [51], and Williams et al. [20], the perceived severity is positively related to behavior [15,19,20,51]. The outcome of this study, as shown in Table 6, supported that perceived severity related to privacy and personal data protection behavior in MCC through perceived threat (b = 0.60, SE = 0.025, p = 0.007).

For Hypothesis 7 (H7), as presented in Table 6, the result of this investigation supported that the perceived susceptibility is positively related to privacy and personal data protection behavior in MCC through perceived threat (b = 0.56, SE = 0.023, p = 0.007). It is interesting to point out that the current finding is consistent with the findings of many studies in the literature that focused on protecting the users of the technologies from security attacks and threats [15,19,20,49–51]. In other words, it's interesting to note that the current outcome is signaling that when vulnerabilities, violations, and threats to privacy and personal data protection are investigated by MCC users, the users will be more likely to take further countermeasures according to their privacy and personal data protection behaviors.

In general, this study's results supported that the perceived benefits, cues to action of PbD, and the perceived threat are positively and directly related to privacy and personal data protection behavior in MCC. Moreover, the results supported that the perceived barriers are negatively and directly related to privacy and personal data protection behavior in MCC. More importantly, the results of this exploration will be beneficial to scholars, managers, and policymakers in helping them for more understanding of the effects of applying PbD to preserve privacy and personal data protection in MCC.

5. Threat to Validity

In this section, we describe and relieve the risks to the validity of this exploratory study. The threat includes internal validity, external validity, and construct validity [86].

5.1. Internal Validity

Internal validity refers specifically to whether an experimental treatment/condition makes a difference or not, and whether there is sufficient evidence to support the claim [87]. For this study, the internal validity is about utilizing the HBM model, the self-reported approach bias, the pilot study, and the sample size.

To mitigate those threats, we utilized the HBM model investigation according to similarly conducted studies [15,19,20,49–51] where those studies and the current research concerning the security issues. Moreover, a self-reported approach is a common approach for gathering the data, since it reduces the possibility of respondents reporting their intention according to what they deem as socially desirable [15]. Moreover, a pilot study was performed in which the questionnaire was distributed to 100 responds who used MCC and who did not participate again in the main study.

Besides, as presented in Hair et al. [69], the sample size of the main study is recommended to be ten times the highest number of structural paths to a latent variable. Accordingly, we validated our model by using survey data based on a sample of 386 responds who used cloud storage in MCC to make sure that our study has strong validity. Our sample is more than related studies in the domain, including the Ng et al. [15] and Williams et al. [20], which are 134 and 237, respectively.

5.2. External Validity

External validity refers to the generalizability of the treatment/condition outcomes [38]. For this study, external validity is about utilizing the visibility and transparency principle out of the seven principles of PbD is a threat to the external validity of the study. This threat is migrated, since investigating one principle in PbD and generalized the results is a common practice in the

research domain [40,88–90]. Moreover, a recent systemic mapping study has revealed that many studies in PbD have studied at least one PbD principle and generalized the results [40].

5.3. Construct Validity

This validity is associated between the theory and the observation in a relationship. If the cause-and-effect relationship is causal, it must ensure the treatment reflects well the cause construct, and the result reflects the effect construct [91].

In this study, the construct validity is about utilizing the HBM to assess preserving privacy and personal data protection in MCC. To mitigate this threat, the HBM is being used in the information systems' security to explain why some people do not perceive a threat sufficient to prompt the adoption of computer security software [49] to assess the influence of security awareness and security technology on users' behavior with regards to health information systems' security [50], to investigate the moderating effect of working experience of health professionals on the relationship between management support and user's ISP compliance behavior [19], and to contribute to a better understanding of the security behavior of computer users in organizations, so that the security environment of an organization can be improved, by identifying and understanding the determinants of computer security behavior [15]. Following that, this study utilized the HBM.

6. Comparison with Related Work

This part presents and related works of this study and demonstrates a comparison of this study with the related works.

Several studies investigated data issues [15,19,20,49–51,56,92,93] related to this study have been carried out in the literature. Ng et al. [15] used the Health Belief Model to study user's computer security behavior. Ng et al. [15] gathered survey data from 134 employees. The results of Ne et al. [15] showed that perceived benefits and perceived susceptibility are determinants of email-related security behavior. Claar et al. [49] proposed a conceptual framework that used the Health Belief Model to explain why some people are not aware of a threat sufficient to induce the adoption of computer security software.

Moreover, Humaidi et al. [50] utilized interviews, questionnaires, and surveys to assess the effect of security technology and security awareness on users' behavior in relation to health information systems' security based on the HBM and Protection Motivation Theory. Humaidi et al. [19] explored the moderate effect of the health professional's working experience on the relationship between factors of the Health Information System Security Policies Compliance Behavior (HISSPC) model. The model [19] was tested by using the partial least squares (PLS) approach with outcomes pointing to the coefficient of determination (i.e., R^2).

Besides, Williams et al. [20] developed a model named the security belief model, which is built from existing models of health behavior is established to explain information security behavior intentions. Williams et al. [20] empirically tested the model based on a sample of 237 professionals. The results [20] point to the general support for their model, especially susceptibility, severity, benefits, and a cue to action as antecedents to the intention to perform preventive information security behaviors [20].

In addition, Dodel et al. [56] presented a cyber-victimization preventive behavior utilizing the HBM. Dodel et al. [56] demonstrated a conceptual model on the determinants of non-digital preventive actions. Dodel et al. [56] investigated the determinants of cyber-safety activities, especially the factors linked with the use of anti-virus software on the Internet with the users. The results of Dodel et al. [56] demonstrated the role of attitudes and values in the reduction of online threats.

Moreover, Koloseni et al. [51] utilized the HBM to investigate employees' security behaviors, especially both automatic or habitual security behaviors and conscious security behaviors of Tanzanian government employees. The results of the research [51] supported that perceived barriers, perceived severity, perceived susceptibility, and cues to the action and security habits affected the intentions of government employees to practice information security behavior [51].

Additionally, Schymik et al. [92] seek to determine the email security behaviors of undergraduate students. A survey was utilized, and a questionnaire was developed based on the HBM [92]. The study [92] supported that the perceived benefits are affecting students' security behavior. Furthermore, Ameme et al. [93] attempt to explain the reasons behind security breaches and developed a model using the HBM for predicting the behaviors of internet banking customers'. Ameme et al. [93] reported a relationship between internet banking security breaches and customer behaviors. The authors [93] mentioned that their outcome has significant policy implications for banks, which help to understand the behavior of customers on internet banking platforms.

In summary, Table 7 presents a comparison between this study and related works of this study. Table 7 shows the reference number of each study, year, research type, contribution type, whether the study used the HBM or not, and whether it used PbD. The contribution type facet is referred to as the type of intervention being studied [94].

Table 7. A comparison between this work and the related works.

Reference Number	Year	Main Issue	Contribution Type Facet	HBM Used.	PbD Used
[15]	2009	User's computer security behaviors.	Model	Yes	No
[49]	2010	Computer security software.	Model	Yes	No
[50]	2012	Health information systems' security.	Framework	Yes	No
[20]	2014	Information security behavior intentions.	Model	Yes	No
[19]	2015	Health Information System Security.	Model	Yes	No
[93]	2016	The reasons behind security breaches.	Model	Yes	No
[56]	2017	Cyber-safety activities.	Model	Yes	No
[92]	2017	Email security behaviors.	Model	Yes	No
[51]	2019	Security behaviors of employees.	Model	Yes	No
This study	2020	Privacy and Personal Data Protection in MCC	Framework	Yes	Yes

As presented in Table 7, 9 studies are related to this study; the studies were conducted in the years from 2009 to 2019. Table 7 revealed that most related works were undertaken in security, such as security behaviors, behavior intentions, security breaches, and Cyber-safety activities. Moreover, in the contribution type facets, most of the studies are producing models, except in 2012, research had a framework. Furthermore, all related studies utilized the HBM, and none of them are using the PbD.

7. Conclusions

Mobile technology is widespread media of data storage, including sensitive information. Due to the limitation in mobile devices, users migrate their data to cloud storage. MCC is a domain resulted from advances in mobile technology and cloud computing [22]. Privacy and protection of MCC data are increasingly recognized as one of the key data issues to protect MCC users [11,12,95]. This study explored the effects of applying PbD to preserve privacy and personal data protection in MCC.

In this study, a framework using PbD has been demonstrated, and seven hypotheses were formulated by adopting the HBM. To test the hypotheses, a survey has been implemented where a questionnaire has been circulated, and a pilot study has been conducted with 100 responses. Moreover, a total of 386 responses were used for the current analysis.

The results of this study supported that the perceived benefits, cues to action of PbD, and the perceived threat is positively and directly affected privacy and personal data protection behavior in MCC. Moreover, the results supported that the perceived barriers are negatively and directly affected privacy and personal data protection behavior in MCC.

More broadly, not only the privacy issues affecting individuals, but also organizations, and when dealing with organizations, there is also a matter of security [96]. Therefore, in conclusion, we believe that applying PbD for MCC is crucial for both users, private organizations, and public organizations. To conclude, this study's results will help researchers and practitioners, including managers and policymakers, with the necessary perception when utilizing PbD to preserve privacy and personal data

protection in MCC Moreover, the results of this exploration supported and encouraged the utilization of PbD to preserve privacy and personal data protection in MCC.

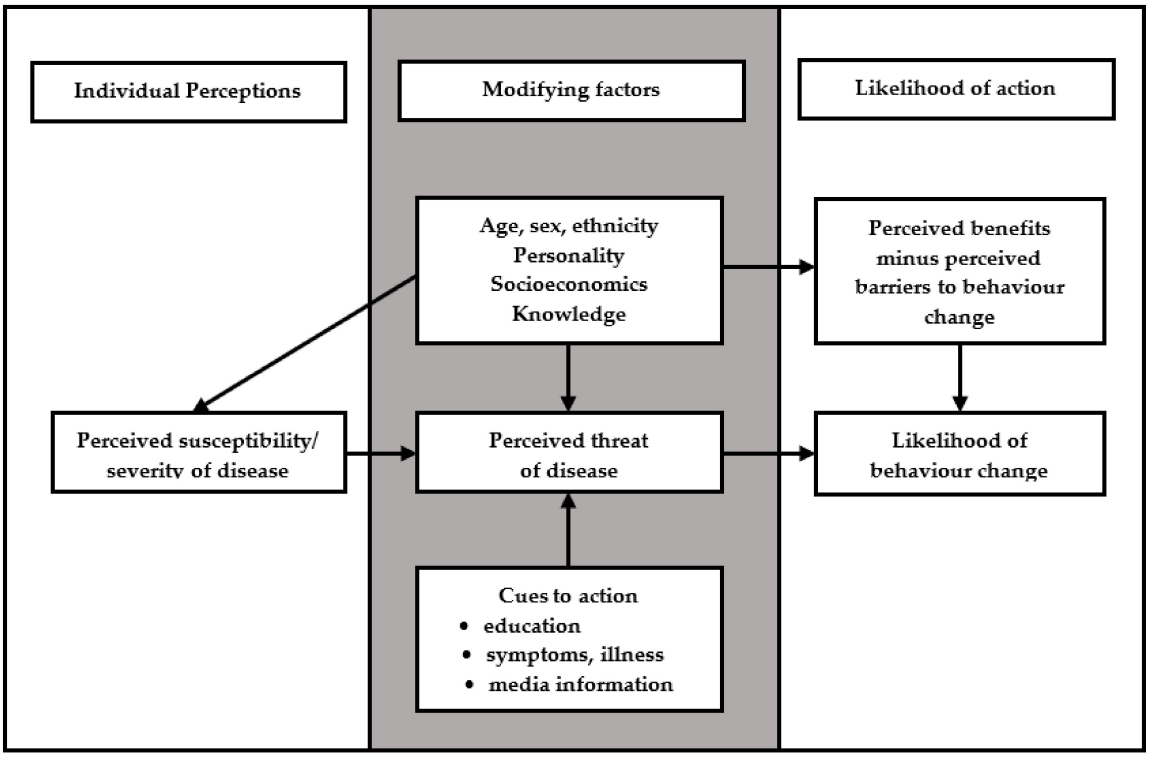
Author Contributions: H.M.A.: Conceptualization, Investigation, Methodology, Software, Validation, Visualization, Writing—original draft, Writing—review & editing, A.A.N.: Supervision, Conceptualization, Investigation, Methodology, Project administration, Resources, Software, Validation, Writing—original draft, Writing—review & editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The Health Belief Model Adapted from Rosenstock, 1974 [18].



Appendix B

Examples of privacy issues presented in the literature.

#	Threat	Explanation
1	Phishing Attacks	"is a type of fraudulent attack in which the intruder acquires the user's personal information by masquerading as a trustworthy third party through either a fake or stolen identity." [97].
2	Spam Attacks	Spam messages are unwanted messages.
3	Information Leakage	"Social media are all about openly sharing and exchanging information with friends. Some users willingly share their personal information such as health-related data." [97].
4	Location Leakage threat	is a type of data leakage [97].
5	Cyberstalking	"is to harass an individual or group through the Internet or social networking." [97].

#	Threat	Explanation
6	User Profiling	"is one of the common activities in almost all online services, where OSN servers analyze routine user activities in their space through various machine-learning techniques." [97].
7	Surveillance	"is a new type of monitoring that is different from the sociability and social roles of a person in politics, the economy, and civil society." [97].
8	User identification	"is defined as a feature that helps individuals recognize each other." [98].
9	Privacy of user's personal space	"The visibility of a social profile has a different type of presence on different social networks." [98].
10	Users' communication	The information that a user shares with other online social network users, for example, there is some default information that a user shares with the online social network provider such as visited profiles, IP address, the time of connection, and the messages sent. [98].

References

1. Asrani, P. Mobile cloud computing. *Int. J. Eng. Adv. Technol.* **2013**, *2*, 606–609.
2. Alnajrani, H.M.; Norman, A.A.; Ahmed, B.H. Privacy and data protection in mobile cloud computing: A systematic mapping study. *PLoS ONE* **2020**, *15*. [CrossRef] [PubMed]
3. Sandle, P. Reuters. British Airways Faces Record $230 Million Fine Over Data Theft. 2019. Available online: https://www.reuters.com/article/us-iag-cybercrime-ico/british-airwaysfaces-record-230-million-fine-over-data-theft-idUSKCN1U30KD (accessed on 12 November 2020).
4. Cappa, F.; Oriani, R.; Peruffo, E.; McCarthy, I. Big Data for Creating and Capturing Value in the Digitalized Environment: Unpacking the Effects of Volume, Variety, and Veracity on Firm Performance. *J. Prod. Innov. Manag.* **2020**. [CrossRef]
5. Arthur, C. The Guardian. DigiNotar SSL Certificate Hack Amounts to Cyberwar, Says Expert. 2011. Available online: http://www.theguardian.com/technology/2011/sep/05/diginotar-certificate-hack-cyberwar (accessed on 15 November 2020).
6. Ryan, M.D. Cloud computing privacy concerns on our doorstep. *Commun. ACM* **2011**, *54*, 36–38. [CrossRef]
7. Hsu, H.M. Does Privacy Threat Matter in Mobile Health Service? From Health Belief Model Perspective. In *PACIS 2016 Proceedings*; Pacific Asia Conference on Information Systems (PACIS): Atlanta, GA, USA, 2016; p. 65.
8. Del Vecchio, P.; Mele, G.; Passiante, G.; Vrontis, D.; Fanuli, C. Detecting customers knowledge from social media big data: Toward an integrated methodological framework based on netnography and business analytics. *J. Knowl. Manag.* **2020**, *24*, 799–821. [CrossRef]
9. Finn, R.L.; Wright, D.; Friedewald, M. Seven types of privacy. In *European Data Protection: Coming of Age*; Springer: Dordrecht, The Netherlands, 2013; pp. 3–32.
10. Hayes, D.R.; Cappa, F. Open-source intelligence for risk assessment. *Bus. Horiz.* **2018**, *61*, 689–697. [CrossRef]
11. Pearson, S.; Yee, G. *Privacy and Security for Cloud Computing: Computer Communications and Networks*; Springer: London, UK, 2013.
12. Alnemr, R.; Cayirci, E.; Dalla Corte, L.; Garaga, A.; Leenes, R.; Mhungu, R.; Pearson, S.; Reed, C.; de Oliveira, A.S.; Stefanatou, D.; et al. A data protection impact assessment methodology for cloud. In *Annual Privacy Forum*; Springer: Cham, Switzerland, 2015; pp. 60–92.
13. Dove, E.S. The EU General Data Protection Regulation: Implications for international scientific research in the digital era. *J. Law Med. Eth.* **2018**, *46*, 1013–1030. [CrossRef]
14. Kroener, I.; Wright, D. A strategy for operationalizing privacy by design. *Inf. Soc.* **2014**, *30*, 355–365. [CrossRef]
15. Ng, B.Y.; Kankanhalli, A.; Xu, Y.C. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
16. Edwards, K. Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA, 2015.

17. Orji, R.; Vassileva, J.; Mandryk, R. Towards an effective health interventions design: An extension of the health belief model. *Online J. Public Health Inform.* **2012**, *4*. [CrossRef]
18. Rosenstock, I.M. Historical origins of the health belief model. *Health Educ. Monogr.* **1974**, *2*, 328–335. [CrossRef]
19. Humaidi, N.; Balakrishnan, V. The moderating effect of working experience on health information system security policies compliance behaviour. *Malays. J. Comput. Sci.* **2015**, *28*, 70–92.
20. Williams, C.K.; Wynn, D.; Madupalli, R.; Karahanna, E.; Duncan, B.K. Explaining users' security behaviors with the security belief model. *J. Organ. End User Comput.* **2014**, *26*, 23–46. [CrossRef]
21. Ringle, C.M.; Wende, S.; Will, A. *SmartPLS*; Version 2.0 M3; University of Hamburg: Hamburg, Germany, 2005.
22. Ferreira, J.A.L.; da Silva, A.R. Mobile cloud computing. *Open J. Mob. Comput. Cloud Comput.* **2014**, *1*, 59–77.
23. Al-Ruithe, M.; Benkhelifa, E.; Hameed, K. Current state of cloud computing adoption–an empirical study in major public sector organizations of saudi arabia (ksa). *Procedia Comput. Sci.* **2017**, *110*, 378–385. [CrossRef]
24. Fernando, N.; Loke, S.W.; Rahayu, W. Mobile cloud computing: A survey. *Future Gener. Comput. Syst.* **2013**, *29*, 84–106. [CrossRef]
25. Bellman, S.; Johnson, E.J.; Kobrin, S.J.; Lohse, G.L. International differences in information privacy concerns: A global survey of consumers. *Inf. Soc.* **2004**, *20*, 313–324. [CrossRef]
26. Tikkinen-Piri, C.; Rohunen, A.; Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Comput. Law Secur. Rev.* **2018**, *34*, 134–153. [CrossRef]
27. Fromholz, J.M. The European Union data privacy directive. *Berk. Tech. LJ* **2000**, *15*, 461.
28. Harfoushi, O. Trust model for effective cloud computing usage: A quantitative study. *J. Theor. Appl. Inf. Technol.* **2017**, *95*, 1116–1123.
29. Ruiter, J.; Warnier, M. Privacy regulations for cloud computing: Compliance and implementation in theory and practice. In *Computers, Privacy and Data Protection: An Element of Choice*; Springer: Dordrecht, The Netherlands, 2011; pp. 361–376.
30. Hanen, J.; Kechaou, Z.; Ayed, M.B. An enhanced healthcare system in mobile cloud computing environment. *Vietnam J. Comput. Sci.* **2016**, *3*, 267–277. [CrossRef]
31. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In *Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012*; IEEE: New York, NY, USA, 2012; Volume 1, pp. 647–651.
32. Guilloteau, S.; Venkatesen, M. *Privacy in Cloud Computing-ITU-T Technology Watch Report March 2012*; International Telecommunication Union: Geneva, Switzerland, 2013.
33. Langheinrich, M. Privacy by design—Principles of privacy-aware ubiquitous systems. In *Proceedings of the International Conference on Ubiquitous Computing, Atlanta, GA, USA, 30 September–2 October 2001*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 73–291.
34. Baharon, M.R.; Shi, Q.; Llewellyn-Jones, D. A new lightweight homomorphic encryption scheme for mobile cloud computing. In *Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015*; IEEE: New York, NY, USA, 2015; pp. 618–625.
35. Angin, P.; Bhargava, B.; Ranchal, R.; Singh, N.; Linderman, M.; Othmane, L.B.; Lilien, L. An entity-centric approach for privacy and identity management in cloud computing. In *Proceedings of the 2010 29th IEEE Symposium on Reliable Distributed Systems, New Delhi, India, 31 October–3 November 2010*; IEEE: New York, NY, USA, 2010; pp. 177–183.
36. Huang, D.; Zhou, Z.; Xu, L.; Xing, T.; Zhong, Y. Secure data processing framework for mobile cloud computing. In *Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011*; IEEE: New York, NY, USA, 2011; pp. 614–618.
37. Li, F.; Rahulamathavan, Y.; Conti, M.; Rajarajan, M. Robust access control framework for mobile cloud computing network. *Comput. Commun.* **2015**, *68*, 61–72. [CrossRef]
38. Douglas, J.E.; Burgess, A.W.; Burgess, A.G.; Ressler, R.K. *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime*; John Wiley & Sons: New York, NY, USA, 2013.
39. Maurushat, A. *Ethical Hacking*; University of Ottawa Press: Ottawa, ON, Canada, 2019.
40. Ehécatl Morales-Trujillo, M.; García-Mireles, G.A.; Matla-Cruz, E.O.; Piattini, M. A Systematic Mapping Study on Privacy by Design in Software Engineering. *CLEI Electron. J.* **2019**, *22*. [CrossRef]
41. Le Métayer, D. Privacy by design: A matter of choice. In *Data Protection in a Profiled World*; Springer: Dordrecht, The Netherlands, 2010; pp. 323–334.

42. Sanaei, Z.; Abolfazli, S.; Gani, A.; Buyya, R. Heterogeneity in mobile cloud computing: Taxonomy and open challenges. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 369–392. [CrossRef]
43. Abolfazli, S.; Sanaei, Z.; Gani, A.; Xia, F.; Yang, L.T. Rich mobile applications: Genesis, taxonomy, and open issues. *J. Netw. Comput. Appl.* **2014**, *40*, 345–362. [CrossRef]
44. Flores, H.; Srirama, S.N.; Paniagua, C. A Generic Middleware Framework for Handling Process Intensive Hybrid Cloud Services from Mobiles. Available online: http://doi.acm.org/10.1145/2095697.2095715 (accessed on 11 November 2020).
45. Cui, Y.; Lai, Z.; Wang, X.; Dai, N. Quicksync: Improving synchronization efficiency for mobile cloud storage services. *IEEE Trans. Mob. Comput.* **2017**, *16*, 3513–3526. [CrossRef]
46. Jayanti, R.K.; Burns, A.C. The antecedents of preventive health care behavior: An empirical study. *J. Acad. Mark. Sci.* **1998**, *26*, 6–15. [CrossRef]
47. Ng, B.Y.; Xu, Y. Studying users' computer security behavior using the Health Belief Model. In Proceedings of the Conference: Pacific Asia Conference on Information Systems, PACIS 2007, Auckland, New Zealand, 4–6 July 2007.
48. Humaidi, N. An Investigation of Health Information System Security Policies Compliance Behaviour. Ph.D. Dissertation, University of Malaya, Kuala Lumpur, Malaysia, 2016.
49. Claar, C.L.; Johnson, J. Analyzing the adoption of computer security utilizing the Health Belief Model. *Issues Inf. Syst.* **2010**, *11*, 286–291.
50. Humaidi, N.; Balakrishnan, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR*; IACSIT Press: Singapore, 2012; Volume 35, pp. 1–6.
51. Koloseni, D.N.; Lee, C.Y.; Gan, M.L. Understanding Information Security Behaviours of Tanzanian Government Employees: A Health Belief Model Perspective. *Int. J. Technol. Hum. Interact.* **2019**, *15*, 15–32. [CrossRef]
52. Davis, F.D. A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. Ph.D. Dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 1985.
53. Goldenhar, L.M.; Connell, C.M. Understanding and predicting recycling behavior: An application of the theory of reasoned action. *J. Environ. Syst.* **1992**, *22*, 91–103. [CrossRef]
54. Lee, J.; Cerreto, F.A.; Lee, J. Theory of planned behavior and teachers' decisions regarding use of educational technology. *J. Educ. Technol. Soc.* **2010**, *13*, 152–164.
55. Vatka, M. *Information Behaviour and Data Security: Health Belief Model Perspective*; Åbo Akademi: Turku, Finland, 2019.
56. Dodel, M.; Mesch, G. Cyber-victimization preventive behavior: A health belief model approach. *Comput. Hum. Behav.* **2017**, *68*, 359–367. [CrossRef]
57. Glanz, K.; Rimer, B.K.; Viswanath, K. *Health Behavior and Health Education: Theory, Research, and Practice*; John Wiley & Son: New York, NY, USA, 2008.
58. Wetzels, M.; Odekerken-Schröder, G.; Van Oppen, C. Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Q.* **2009**, 177–195. [CrossRef]
59. Al Khater, N.R. A Model of a Private Sector Organisation's Intention to Adopt Cloud Computing in the Kingdom of Saudi Arabia. Ph.D. Dissertation, University of Southampton, Southampton, UK, 2017.
60. Brown, S. *Likert Scale Examples for Surveys. ANR Program Evaluation*; Iowa State University: Ames, IA, USA, 2010.
61. Vasantha, R.N.; Harinarayana, N.S. Online survey tools: A case study of Google Forms. In *National Conference on Scientific, Computational & Information Research Trends in Engineering, GSSS-IETW, Mysore*; University in Mysore: Mysore, India, 2016.
62. Petrić, B.; Czárl, B. Validating a writing strategy questionnaire. *System* **2003**, *31*, 187–215. [CrossRef]
63. Wallace, L.S.; Blake, G.H.; Parham, J.S.; Baldridge, R.E. Development and content validation of family practice residency recruitment questionnaires. *Fam. Med. Kans. City* **2003**, *35*, 496–498.
64. Esmaeili, M. Assessment of Users' Information Security Behavior in Smartphone Networks. Ph.D. Thesis, Eastern Michigan University, Ypsilanti, MI, USA, 2014.
65. Hassan, Z.A.; Schattner, P.; Mazza, D. Doing a pilot study: Why is it essential? *Malays. Fam. Physician* **2006**, *1*, 70–73.
66. Tumusiime, D.K. Perceived Benefits of, Barriers and Helpful Cues to Physical Activity among Tertiary Institution Students in Rwanda. Ph.D. Dissertation, University of the Western Cape, Cape Town, South Africa, 2004.

67. Tongco, M.D.C. Purposive sampling as a tool for informant selection. *Ethnobot. Res. Appl.* **2007**, *5*, 147–158. [CrossRef]
68. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E.; Tatham, R. *Multivariate Data Analysis*; Prentice hall Upper Saddle River: Bergen, NJ, USA, 1998.
69. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a silver bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–152. [CrossRef]
70. Creswell, J.W. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*; Pearson: London, UK, 2012.
71. Nulty, D.D. The adequacy of response rates to online and paper surveys: What can be done? *Assess. Eval. Higher Educ.* **2008**, *33*, 301–314. [CrossRef]
72. Saldivar, M.G. A Primer on Survey Response Rate. Ph.D. Thesis, Learning Systems Institute Florida State University, Tallahassee, FL, USA, 2012.
73. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
74. Chin, W.W. The partial least squares approach to structural equation modeling. *Modern Methods Bus. Res.* **1998**, *295*, 295–336.
75. Ab Hamid, M.R.; Sami, W.; Sidek, M.M. Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In *Journal of Physics: Conference Series*; IOP Science: Bristol, UK, 2017; Volume 890.
76. Janadari, M.P.N.; Sri Ramalu, S.; Wei, C. Evaluation of measurment and structural model of the reflective model constructs in PLS–SEM. In Proceedings of the 6th International Symposium—2016 South Eastern University of Sri Lanka (SEUSL), Oluvil, Sri Lanka, 20–21 December 2016.
77. Chin, W.W. How to write up and report PLS analyses. In *Handbook of Partial Least Squares Concepts, Methods and Applications*; Esposito Vinzi, V., Chin, W., Henseler, J., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 655–690.
78. Nunnally, J.C. *Psychometric Theory*, 2nd ed.; McGraw-Hill: Singapore, 1978.
79. Hair, J.F.; Babin, B.J.; Black, W.C. *Multivariate Data Analysis: A Global Perspective*, 7th ed.; Pearson Education: London, UK, 2010.
80. Petter, S.; Straub, D.; Rai, A. Specifying formative constructs in information systems research. *MIS Q.* **2007**, 623–656. [CrossRef]
81. Bagozzi, R.P.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1988**, *16*, 74–94. [CrossRef]
82. Gefen, D.; Straub, D. A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Commun. Assoc. Inf. Syst.* **2005**, *16*. [CrossRef]
83. Gefen, D.; Straub, D.; Boudreau, M.C. Structural equation modeling and regression: Guidelines for research practice. *Commun. Assoc. Inf. Syst.* **2000**, *4*. [CrossRef]
84. Falk, R.F.; Miller, N.B. *A Primer for Soft Modeling*; University of Akron Press: Akron, OH, USA, 1992.
85. Puspita, R.C.; Tamtomo, D.; Indarto, D. Health belief model for the analysis of factors affecting hypertension preventive behavior among adolescents in Surakarta. *J. Health Promot. Behav.* **2017**, *2*, 183–196. [CrossRef]
86. Ahmed, B.H.; Lee, S.P.; Su, M.T. The Effects of Static Analysis for Dynamic Software Updating: An Exploratory Study. *IEEE Access* **2020**, *8*, 35161–35171. [CrossRef]
87. Khorsan, R.; Crawford, C. External validity and model validity: A conceptual approach for systematic review methodology. *Evid. Based Complement. Altern. Med.* **2014**, *2014*. [CrossRef]
88. Cavoukian, A.; Fisher, A.; Killen, S.; Hoffman, D.A. Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design. *Identity Inf. Soc.* **2010**, *3*, 363–378. [CrossRef]
89. Cavoukian, A. *Global Privacy and Security, by Design: Turning the "Privacy vs. Security" Paradigm on its Head*; Springer: Cham, Switzerland, 2017.
90. Cavoukian, A.; Spencer, P.C. *The Ontario Health Study's Assessment Centres: A Case Study for "Privacy by Design"*; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2010.
91. Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.C.; Regnell, B.; Wesslén, A. *Experimentation in Software Engineering*; Springer Science & Business Media: Berlin, Germany, 2012.
92. Schymik, G.; Du, J. Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model. In *Proceedings of the Conference on Information Systems Applied Research ISSN*; ISCAP: São Mamede de Infesta, Portugal, 2017; Volume 2167, p. 1508.

93. Ameme, B.K.; Yeboah-Boateng, E.O. Internet Banking Security Concerns: An Exploratory Study of Customer Behaviors Based on Health Belief Model. Available online: https://www.researchgate.net/publication/298794389 (accessed on 20 November 2020).
94. Ahmed, B.H.; Lee, S.P.; Su, M.T.; Zakari, A. Dynamic software updating: A systematic mapping study. *IET Softw.* **2020**, *14*, 468–481. [CrossRef]
95. Dey, S.; Sampalli, S.; Ye, Q. Security and privacy issues in mobile cloud computing. *Int. J. Bus. Cyber Secur.* **2016**, *1*, 31–43.
96. Hayes, D.; Cappa, F.; Le-Khac, N.A. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. *Dig. Bus.* **2020**, *1*. [CrossRef]
97. Ali, S.; Islam, N.; Rauf, A.; Din, I.U.; Guizani, M.; Rodrigues, J.J. Privacy and security issues in online social networks. *Future Internet* **2018**, *10*, 114. [CrossRef]
98. Al-Muhtadi, J.; Shahzad, B.; Saleem, K.; Jameel, W.; Orgun, M.A. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Inform. J.* **2019**, *25*, 315–329. [CrossRef]