PRIVACY-BY-DESIGN FRAMEWORK FOR PRIVACY AND PERSONAL DATA PROTECTION IN MOBILE CLOUD COMPUTING

ALNAJRANI, HUSSAIN MUTLAQ H

FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITI MALAYA
KUALA LUMPUR

2022

PRIVACY-BY-DESIGN FRAMEWORK FOR PRIVACY AND PERSONAL DATA PROTECTION IN MOBILE CLOUD COMPUTING

ALNAJRANI, HUSSAIN MUTLAQ H

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITI MALAYA
KUALA LUMPUR

2022

UNIVERSITI MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **ALNAJRANI, HUSSAIN MUTLAQ H.**

Matric No: (**WHA 160049 / 17043351/1)**

Name of Degree: **Doctor of Philosophy (PhD)**

Title of Thesis: **PRIVACY-BY-DESIGN FRAMEWORK FOR PRIVACY AND PERSONAL DATA PROTECTION IN MOBILE CLOUD COMPUTING**

Field of Study: **INFORMATION SYSTEMS SECURITY (MOBILE CLOUD COMPUTING)**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 11 November 2021

Subscribed and solemnly declared before,

Witness's Signature

Date: 11 November 2021

Name:

Designation:

PRIVACY-BY-DESIGN FRAMEWORK FOR PRIVACY AND PERSONAL DATA PROTECTION IN MOBILE CLOUD COMPUTING

ABSTRACT

As an outcome of a shift in technology, Mobile Cloud Computing (MCC) has been established using the combination of universal mobile networks and cloud computing. Currently, users move their data to cloud storage due to the limitations of mobile devices. As a result of the significant concern of MCC users, privacy and personal data protection are receiving significant attention in the domain. Privacy and personal data protection are increasingly recognized as key security issues in the domain. Several studies on MCC have been done with attention to privacy and personal data protection. Despite this advancement, no single study developed a Privacy by Design (PbD) framework to preserve Privacy and Personal Data Protection (PPDP) in mobile cloud computing. 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 Information Technology (IT) systems. This thesis aims to develop a PbD framework to preserve PPDP in MCC. In the literature review, a systematic mapping study (SMS) was conducted, and a systematic literature review (SLR) was applied. The SMS identified existing threats and attacks on data privacy, and privacy solutions were proposed on PPDP in MCC. The SLR determined the determinants that influence the preservation of PPDP in MCC. In this research, a framework is projected to preserve PPDP in mobile cloud computing, utilizing PbD. The proposed framework uses PbD visibility and transparency by considering location transparency, laws, and regulations. A survey was conducted to test the formulated hypotheses. In the survey, a questionnaire was circulated and a pilot test with 100 responses was conducted along with the real data collection where 386 responses were received. Both studies utilized the SmartPLS for analysis. The SmartPLS analysis tool was chosen since it is a distinguished software implementation for Partial Least

Squares Structural Equation Modeling (PLS-SEM). The results of this research supported the articulated hypothesis (SE = 0.056, β = 0.552, p = 0.000) 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. Furthermore, the outcomes of this research supported the formulated hypothesis (Standard error (SE) =0.001, Sample Beta (β) = 0.003, P-value (p) =0.015) that cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to the perceived threat. The result will help to determine the PbD framework to preserve privacy and personal data protection in MCC, showing the relation of the perceived threat with privacy and personal data protection behavior in mobile cloud computing, the relation between cues to action with privacy and personal data protection behavior in MCC, and the relation of cues to action with the perceived threat.

Keywords: Privacy by Design, Privacy, Personal Data Protection, Mobile Cloud Computing.

KERANGKA PRIVASI BERASASKAN REKABENTUK UNTUK PRIVASI DAN PERLINDUNGAN DATA PERIBADI DI PENGKOMPUTERAN AWAN MUDAH ALIH

ABSTRAK

Sebagai hasil daripada peralihan teknologi, Pengkomputeran Awan Mudah Alih (MCC) telah ditubuhkan menggunakan gabungan rangkaian mudah alih universal dan pengkomputeran awan. Pada masa ini, pengguna mengalihkan data mereka ke storan awan kerana batasan peranti elektronik mudah alih. Hasil daripada kebimbangan ketara pengguna MCC, privasi dan perlindungan data peribadi menerima perhatian penting dalam domain tersebut. Privasi dan perlindungan data peribadi semakin diiktiraf sebagai isu keselamatan utama dalam domain. Banyak kajian tentang MCC telah dilakukan dengan memberi perhatian kepada privasi dan perlindungan data peribadi. Walaupun kemajuan ini, tiada kajian tunggal membangunkan rangka kerja Privasi oleh Reka Bentuk (PbD) untuk memelihara Privasi dan Perlindungan Data Peribadi (PPDP) dalam pengkomputeran awan mudah alih. PbD ialah falsafah umum yang menunjukkan privasi tidak dilihat secara keseluruhan sebagai sesuatu yang difikirkan kemudian tetapi sebagai keperluan kelas pertama dalam reka bentuk sistem Teknologi Maklumat (IT). Tesis ini bertujuan untuk membangunkan rangka kerja PbD untuk memelihara PPDP dalam MCC. Dalam kajian literatur, kajian pemetaan sistematik (SMS) telah dijalankan, dan kajian literatur sistematik (SLR) telah digunakan. SMS tersebut mengenal pasti serangan dan ancaman sedia ada terhadap privasi data dan penyelesaian privasi yang dicadangkan kepada PPDP dalam MCC. SLR menentukan penentu yang mempengaruhi penyelenggaraan PPDP dalam pengkomputeran awan mudah alih. Dalam penyelidikan ini, rangka kerja diunjurkan untuk mengekalkan PPDP dalam pengkomputeran awan mudah alih, menggunakan PbD. Rangka kerja yang dicadangkan menggunakan keterlihatan dan ketelusan PbD dengan mempertimbangkan ketelusan lokasi, undang-

undang dan peraturan. Tinjauan telah dijalankan untuk menguji hipotesis yang dirumus. Dalam tinjauan tersebut, soal selidik telah diedarkan, ujian rintis dengan 100 respons telah dijalankan dan diikuti dengan pengumpulan data sebenar di mana 386 respons telah diterima. Kedua-dua kajian menggunakan SmartPLS untuk analisis. SmartPLS adalah satu implementasi perisian yang terkenal untuk Pemodelan Persamaan Struktur Kuasa Dua Separa Terkecil (PLS-SEM). Keputusan penyelidikan ini menyokong hipotesis yang diartikulasikan (SE = 0.056, β = 0.552, p = 0.000) yang memberi petunjuk kepada tindakan PbD memandangkan ketelusan lokasi keterlihatan, undang-undang dan peraturan berkaitan secara positif dengan privasi dan tingkah laku perlindungan data peribadi dalam pengkomputeran awan mudah alih. Tambahan pula, hasil penyelidikan ini menyokong hipotesis yang dirumuskan (Ralat piawai (SE) =0.001, Sampel Beta (β) = 0.003, nilai P (p) =0.015) yang memberi petunjuk kepada tindakan privasi dengan reka bentuk mempertimbangkan ketelusan lokasi keterlihatan, undang-undang dan peraturan berkaitan secara positif dengan ancaman tanggapan. Hasilnya akan membantu menentukan kerangka PbD untuk menjaga privasi dan perlindungan data peribadi dalam pengkomputeran awan mudah alih, menunjukkan hubungan antara ancaman yang dirasakan terhadap privasi dan tingkah laku perlindungan data peribadi dalam MCC, hubungan antara privasi dan isyarat perilaku perlindungan data peribadi dalam MCC dan hubungan isyarat tindakan dengan ancaman tanggapan.

Kata kunci: Privasi oleh Reka Bentuk, Privasi, Perlindungan Data Peribadi, Pengkomputeran Awan Mudah Alih.

ACKNOWLEDGEMENTS

I would like to convey my intense and earnest appreciation to my respected supervisor, Dr. Azah Anir Norman, for giving me the opportunity and facility to work under her invaluable guidance in conducting my research and providing invaluable and insightful suggestions and advice throughout the research period. Your supervision and advice quickly set the tone, direction, and pace of this research. You ensured that I remained on track and moving forward. This study would probably not have been successful without the support, feedback, and guidance of your supervision. It was a wonderful privilege and respect to work and study under your direct support and guidance.

No words are enough to express my heartfelt gratitude for the love, prayers, and care of my parents from the day I started this research. I am very much thankful to my beloved wife and my lovely kids for their unconditional love, understanding, patience, sacrifices, and consistent support granted to me to complete my research. I also would like to convey big thanks to my adorable brothers and sisters for their harmonious support and prayers. My thanks go to the rest of my family and friends who understand the sacrifices and dedication required to complete this dissertation.

My special thanks go to the University of Malaya management for facilitating me to conduct my research in a unique scientific community, and for this extension to the most knowledgeable staff of the Faculty of Computer Science and Information Technology (CSIT). I am also very thankful to my friends and colleagues for their enthusiastic support all the time.

Finally, I want to dedicate this work to my parents and family for their care, support, and trust in me. They did their best and have invested so much in my success. Thank you so much, Mom, Dad, and my family members. Moreover, many thanks go to those who have motivated and coached me throughout my education and career.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES PAGE

LIST OF TABLES

TABLES PAGE

LIST OF SYMBOLS AND ABBREVIATIONS

AVE	:	Average variance extracted
CA	:	Cronbach's Alpha
CAPD	:	Cue to Action of privacy by design
CC	:	Cloud computing
CR	:	Composite reliability
CSV	:	Comma Separated Values File
CSC	:	Cloud service consumer
CSP	:	Cloud service provider
CV	:	Convergent validity
f^2	:	Effect size
GDPR	:	General Data Protection Regulation
GoF	:	Goodness of Fit of the Model
HBM	:	Health Belief Model
HISSPC	:	Health Information System Security Policies Compliance Behavior
HTMT	:	Heterotrait-Monotrait Ratio
IaaS	:	Infrastructure-as-a-service
IS	:	Information Security
ISS	:	Information Systems security
IT	:	Information Technology
MC	:	Mobile computing
MCC	:	mobile cloud computing
OECD	:	The Organization for Economic Cooperation and Development
PaaS	:	Platform-as-a-Service
PBC	:	Perceived Behavioral Control

PbD	:	Privacy by Design
PPDP	:	Privacy and personal data protection
PDPBMCC	:	Privacy and personal data protection behavior in MCC
PII	:	Personally identifiable information
PLS-SEM	:	Partial Least Squares Structural Equation Modeling
P.BAR	:	Perceived Barriers
P.BEN	:	Perceived Benefits
P.SEV	:	Perceived Severity
P.SUS	:	Perceived Susceptibility
P.Threat	:	Perceived Threat
SaaS	:	Software-as-a-Service
SE	:	Standard error
SMS	:	Systematic mapping study
TAM	:	Technology Acceptance Model
TPB	:	Theory of Planned Behavior
TRA	:	Theory of Reasoned Action
TTAT	:	Technology threat avoidance theory
RO	:	Research objectives
RQ	:	Research questions
R^2	:	R-squared
VIF	:	Variance inflation factor
VM	:	Virtual machine

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.1 Introduction

In the world of technological advancement, various new issues attached to the World Wide Web (WWW) have emerged. There is an improved demand for information security due to the global rise in data breach cases (Weishäupl et al., 2018). Due to constrained inherent in mobile device resources, some users decided to upload mobile content on the internet to save space. There is a phenomenon called Mobile Cloud Computing (MCC) (Stergiou et al., 2018). MCC service is provided to mobile users (Chaubey & Tank, 2016; Asrani, 2013). MCC integrates the features of the mobile network and Cloud Computing (CC) to offer the best services to mobile users. In MCC, all the data and the complex computing modules that may be addressed on the cloud and mobile gadgets do not require robust configurations such as memory capacity and Central Processing Unit (CPU) speed (Somula & Sasikala, 2018; Goyal & Singh, 2014). Despite the convenient nature of this concept, MCC presents numerous challenges for users, specifically concerning the security of their data (Chaubey & Tank, 2016).

With the rise in the popularity of MCC, various firms have undertaken to offer the service, but numerous questions have been raised on how and where these companies store their users' information (Mollah et al., 2017; Zhou & Huang, 2012). The world has become a global village, and these entities are at liberty to set up servers in any country and store user information therein without informing the client (Somula & Sasikala, 2018; Khan et al., 2013). By implementing this, they disregard various vital features such as the predisposition of this country to user data privacy, laws and regulations for cloud computing, and the relationship with the source country (Abd Al Ghaffar, 2020; Wang, 2011). Current research stated that threats, improper policies of security, and privacy that applies in some sites for privacy and personal data protection (PPDP) in MCC cause noncompliance with regulations and laws and threats (Qayyum, 2020; Vatka, 2019;

Baharon et al., 2015; Huang et al., 2011). Specifically, research reported that for mobile users, storing their privacy-sensitive data in a public cloud is a big concern (Huang et al., 2011). In addition, the stored data on the cloud can be located in different places throughout various countries and states, which might be protected in one and not secured in another (Baharon et al., 2015). Interestingly, cloud storage in multiple locations offers critical privacy issues where users' personal information is saved remotely, which may expose their information without their consent (Qayyum, 2020). Moreover, the lack of location privacy may result in disclosing sensitive information about the mobile user (Qayyum, 2020).

In addition, examinations have reported that the threats may include disclosing information or data, data misuse, leakage of user privacy, and identity theft (Ahmad et al., 2018; Han et al., 2018).

1.2 Motivation and Background

This section offers a broad background of MCC, PPDP, and PbD. In addition, this section will introduce the problem statement, research objectives, research questions, significance of the study, thesis organization, and finally, summary of the chapter.

1.2.1 Overview Mobile Cloud Computing

Nowadays, mobile devices like smartphones offer users more accessibility and connection to services and applications (Ferreira & da Silva, 2014). Currently, mobile users have used an accessible internet ability known as Cloud Computing (CC) to save their data. CC offers a powerful method to distribute services via integrating current computer technologies. Thus, this situation generates a new paradigm called Mobile Cloud Computing (MCC) (Stergiou et al., 2018; Fernando et al., 2013). In CC, three service distribution models seem to be accountable for the majority of CC deployments, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) (Kumar et al., 2018).

The notion of MCC arose from combining CC and mobile technologies (Al-Janabi et al., 2017; Juárez & Cedillo, 2017). MCC is a method that provides mobile terminals with robust and authoritative cloud-based computing that allows for the most efficient use of available resources (Somula & Sasikala, 2018). Furthermore, MCC offers chances to better the scalability and portability of services (Somula & Sasikala, 2018; Ferreira & da Silva, 2014).

1.2.1.1 Security and privacy issues in MCC

To link the objectives of this study with security and privacy issues in MCC for a clearer account of how these research objectives were arrived at, it is essential to mention that the primary data security risk arises due to mobile users' data being kept and processed in clouds at service providers' endpoints (Mollah et al., 2017). These threats include data breaches, data locality, data recovery, data loss, and data privacy. Interestingly, data loss and breach violate two security requirements, including integrity and confidentiality (Mollah et al., 2017). The term "data loss" refers to data that has been destroyed or lost by any physical means during processing, transmission, or storage (Mollah et al., 2017). Moreover, a data breach means that the users' data is stolen, used, or copied by unauthorized users (Cheng et al., 2017). Data recovery is another issue that refers to the recovery of data from a mobile user's data that has been failed, damaged, or lost (YAJID, 2017). Furthermore, since users' data is hosted on service providers' premises under cloud service models, customers must know where their data is located or stored, making data locality an issue (Akhtar et al., 2021). Users' data must also be kept distinct from that of others, which will be significantly more susceptible if one user's data mixes, combines, or confounds with that of other users or when data is transferred to the cloud servers to increase storage capacity, where mobile users lose physical control of their data (Mollah et al., 2017). As a result, in a cloud storage environment, data accuracy becomes one of the main issues for mobile users. Even though cloud infrastructures are

much more stable and robust than mobile devices, they face a variety of internal and external risks to data integrity (Mollah et al., 2017).

Besides, privacy is also a significant issue since sensitive data or apps of mobile users are processed and transferred from mobile devices to heterogeneous dispersed cloud servers when using various cloud services, where the service providers' (cloud servers) are situated in various locations and nations (Mollah et al., 2017). Moreover, consumers should know the cloud hosting location since the law varies by region. Additionally, many programs require and collect users' location information, which they may utilize to target customers directly based on their whereabouts. As a result, location-based services pose privacy concerns, as they may collect, store, and analyze user information (Mollah et al., 2017).

1.2.2 Overview of Privacy and Personal Data Protection

Gholami and Laure (2016) defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” (Gholami & Laure, 2016). The concept of privacy is very broad, (Alguliyev et al., 2019) with different points of view based on countries, cultures, or jurisdictions

Several studies have investigated that personal data is "any information relating to an identified or identifiable natural person” (‘data subject’); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Balaji Raykar & Sridhar, 2022). Also, previous researchers have indicated that the main mission of privacy protection is to identify private information based on particular application scenarios and laws (Bansal et al., 2016; Chen & Zhao, 2012).

Privacy is more than hide-out information. It is legal regulation of personal data. No one can obtain personal data without the permission of the owner unless the law permits such access (Kayaalp, 2018) such as income information that can be obtained from employers about their employees by tax authorities (Kayaalp, 2018; Angin et al., 2010).

Privacy issues in MCC have more consideration nowadays; Though several current privacy regulations and laws are required to enforce standards on the disclosure, usage, maintenance, and collection of personal data, and even cloud providers must adhere to these standards (Gellman, 2012). Also, several researchers stated that privacy risks always increase when your data is hosted in hands of someone (Venkatesh & Eastaff, 2018; Gellman, 2012).

For example, as presented in Figure 1.1, the mobile cloud computing user (U) wants to use a mobile cloud service for storing and processing his data whereas cloud service is sited in diverse countries, for example, Country (A) and Country (B). Though, the personal data of the MCC user (U) is conceded to be highly sensitive and requires high privacy. As illustrated in Figure 1.1, the cloud service provider (CSP) is located in an applied General Data Protection Regulation (GDPR), or equivalent to regulations and laws. In contrast, the CSP placed in Country (B) does not use general data protection regulations or anything similar. Consequently, as presented in the literature, the cloud service hosted in a country that doesn't enforce regulations and laws about PPDP in MCC is an issue to privacy violations (data misuse, disclosing information) by a third party (Qayyum, 2020; Maurushat, 2019; Tikkinen-Piri et al., 2018; Harfoushi, 2017; Dey et al., 2016; Ruiter & Warnier, 2011; Bellman et al., 2004; Fromholz, 2000).

In summary, the main issue in the current MCC is the processing of users' personal data in a Country (B) since the MCC provider did not give the MCC user (U) the option of selecting Country A, which is suitable for his/her personal data.

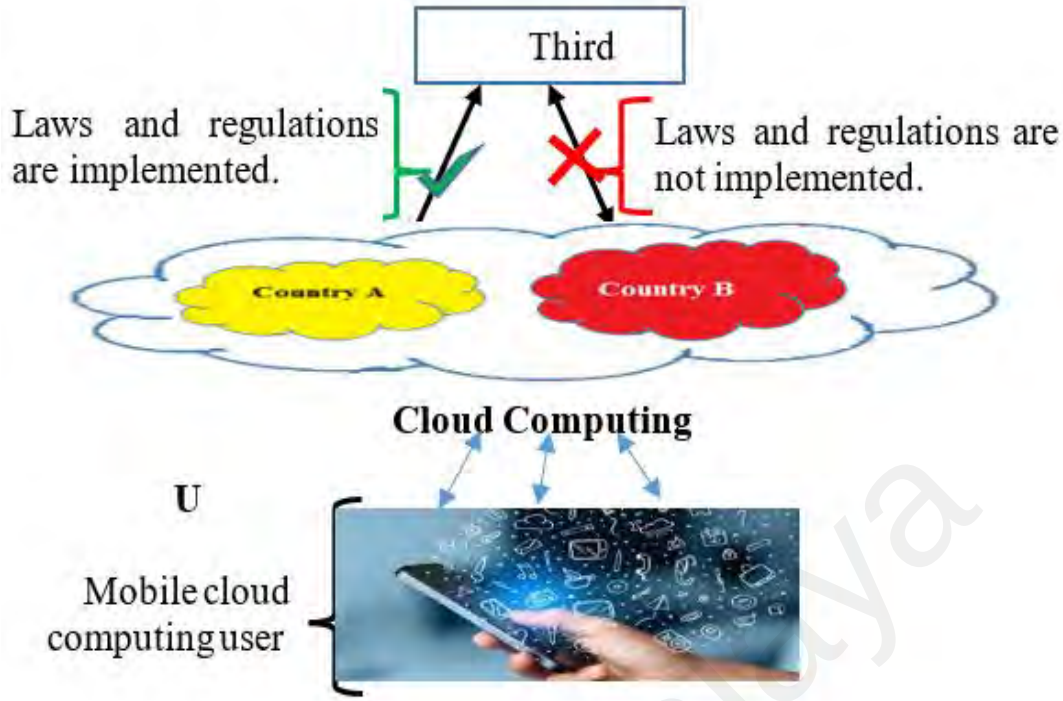


Figure 1.1: Systemic diagram of personal data in MCC

1.2.3 Privacy by Design (PbD)

Recent attention has been concentrated on the provision of privacy by design (PbD), which maintained that all actions performed on a person's data are going with data privacy and security (Shirazi et al., 2017; Kroener & Wright, 2014). Also, PbD is a procedure advised to be used by firms, for instance, CC services providers (Shirazi et al., 2017; Guilloteau & Venkatesen, 2013).

In the literature, several researchers have demonstrated the usage of privacy by design in information security (IS) (Bu et al., 2020; Ross et al., 2019; Cutillo & Lioy, 2013; De Wolf et al., 2013; Islam & Iannella, 2011) and have motivated the researchers to utilize it in the current study. Moreover, even though the discussion regarding appropriate strategies for handling the different challenges of PPDP in mobile cloud computing continues, Privacy by Design (PbD) has not been followed in MCC (Ehécatl Morales-Trujillo et al., 2019). "Privacy by Design (PbD) is a general philosophy that demonstrated that privacy should not be overviewed as an afterthought but rather as a first-class

requirement in the design of Information Technology (IT) systems" (Le Métayer, 2010). Consequently, this study aims to develop a PbD framework to preserve PPDP in MCC.

1.3 Problem Statement

Several studies have shown the usage of cloud computing for storing mobile data (Chaubey & Tank, 2016; Asrani, 2013). As an outcome, privacy and personal data protection (PPDP) in MCC is presently one of the main hurdles in privacy defense issues (Alnemr et al., 2016). For instance, an investigation reported that cloud data might be stored at multiple locations across various countries, which might not be protected in some countries and threatened in others (Baharon et al., 2015). In addition, the landscape of cloud computing has significant implications for the privacy of personal data, including raising questions about the security of the location and who has access to the data in the hosted location (Baharon et al., 2015; Angin et al., 2010), which affects the mobile cloud computing user's choice in utilizing cloud storage (Angin et al., 2010).

Furthermore, questions are raised about attacks and threats to personal data privacy; for instance, studies noted that improper security practices and policies in some locations are one of the issues of PPDP in mobile cloud computing (Qayyum, 2020; Vatka, 2019; Baharon et al., 2015; Li et al., 2015; Huang et al., 2011). Though PPDP in mobile cloud computing may cause laws and regulations noncompliance, as well as attacks and threats such as data misuse, identity theft, disclosing information or data, and leakage of user privacy (Maurushat, 2019; Harfoushi, 2017). It may also jeopardize personal data privacy where the mobile cloud computing users might be exposed to, for example, a spy, social trolling and shaming, taking of the user data, internet viruses, and spam messages (Qayyum, 2020; Maurushat, 2019; Burgess, 2013).

Although discussion remains on the best strategies for dealing with the numerous PPDP issues in mobile cloud computing and to the best of the researcher's knowledge, PbD has not been examined on how to use to preserve PPDP in MCC. "Privacy by Design

(PbD) is a general philosophy that demonstrates that privacy should not be overviewed as an afterthought but rather as a first-class requirement in the design of Information Technology (IT) systems" (Le Métayer, 2010). Consequently, this study aims to develop a PbD framework to preserve privacy and personal data protection in MCC.

1.4 Research Objectives

This study aims to develop a PbD framework to preserve PPDP in MCC. The research objectives (ROs) of this research are as follows:

RO 1: To identify existing data privacy threats and existing solutions proposed to preserve privacy and personal data protection in MCC.

RO 2: To investigate the determinants that influence the preservation of privacy and personal data protection in MCC.

RO 3: To develop privacy by design framework to preserve privacy and personal data protection in MCC.

RO 4: To validate the privacy by design framework in preserving privacy and personal data protection in MCC.

In this thesis, RO 1 has been achieved in Section 2.2 and Section 2.3. Also, RO 2 has been achieved in Subsection 3.3.1. Moreover, RO 3 has been achieved in Section 5.2, and RO 4 has been achieved in Section 5.3.

1.5 Research Questions

To achieve the above research objectives mentioned in Section 1.4, the following research questions (RQs) are formulated:

RQ 1: What are existing privacy threats and existing solutions proposed to preserve privacy and personal data protection in MCC?

RQ 2: What are the determinants that influence the preservation of privacy and personal data protection in MCC?

RQ 3: How to preserve privacy and personal data protection in mobile cloud computing?

RQ 4: How does the PbD framework effects preserving privacy and personal data protection in MCC?

The relation between the research objectives and research questions of this thesis is that each research objective has one research question. Moreover, to explain how those research objectives are achieved, Table 1.1 shows the mapping of the research objectives, research questions, methodology, and expected output.

Table 1.1: Research objectives (ROs), Research questions (RQs), methodology, and expected output

ROs	RQs	Methodology	Expected output
RO 1	**RQ 1**	Quantitative method using SMS. **Phase 1.**	Mapping of current data privacy threats and solutions proposed in mobile cloud computing.
RO 2	**RQ 2**	Quantitative method using SLR. **Phase 1.**	• List of determinants. • Identified theory for research • Proposed PbD framework
RO 3	**RQ 3**	Quantitative. A survey was conducted using SEM-PLS and SmartPLS techniques. **Phase2**	PbD Framework
RO 4	**RQ 4**	Quantitative. Validation analysis Model Fit (R^2, Q^2, F^2, GoF) Using SmartPLS **Phase 3**	Validated PbD Framework

1.6 Significance of this Research

Interestingly, the significance of studying the privacy of MCC comes into the field since mobile devices are more widely used in our daily lives (Wang & Jin, 2019).

Currently, mobile devices are almost in the hand of many MCC users in many places, and the utilization of mobile devices is useful for users generally whenever and wherever they are (Naik & Sarma, 2013). Besides, researchers demonstrated that many mobile devices have a low capacity for storing data (Somula & Sasikala, 2018; Goyal & Singh, 2014). Hence, preserving personal data protection in the mobile cloud has cut the attention of many researchers in the domain.

As presented in Section 1.4, this research aims to develop a PbD framework to preserve PPDP in the MCC. Accordingly, the result of this research will help to preserve PPDP using privacy by design, including the relation of perceived threat with PPDP behavior in the MCC, the relation between cues to action with PPDP behavior in the MCC, and the relation of cues to action with the perceived threat.

The outcomes of this research supported the cues to action of privacy by design, perceived benefits, and perceived threat are positively and directly related to PPDP behavior in the MCC. Besides, the outcomes supported that the perceived barriers are negatively and directly related to PPDP behavior in MCC. In general, the outcome supported the utilization of privacy by design to preserve PPDP in mobile cloud computing, which encourages practitioners to use privacy by design to preserve PPDP in the MCC.

1.7 Thesis Organization

This study contains six chapters, as described below:

Chapter one introduces the research, consisting of the background and motivation that includes MCC, PPDP, and PbD. Also, this chapter has introduced the problem statement, research objectives, research questions, significance of the study, thesis organization, and chapter summary.

Chapter two shows a comprehensive literature review about mobile cloud computing, which includes the background of MCC, the concept of MCC, major actors in MCC,

services of cloud computing, the high-level architecture of MCC, enterprise architecture, and information systems security in MCC. Also, this chapter reviews PPDP, which includes the concept of data privacy, privacy laws, and personal data protection. Moreover, this chapter reviews the existing threats and attacks in mobile cloud computing, privacy solutions projected to preserve personal data protection in MCC, and related work in information systems security and privacy. Furthermore, this chapter presents the research gap of PPDP in the MCC, PbD, and finally, the summary of the chapter.

Chapter three introduces a theoretical perspective of this research. It presents the theoretical perspective of PPDP in the MCC and theories used in research for information systems security and privacy, including the Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), and Health Belief Model (HBM), which includes History of health belief model, HBM assumptions, HBM components, and HBM concepts. Also, this chapter presents a comparative analysis of theories or models, including a summary of theories in information systems security and privacy. In addition, this chapter presents determinants of preserving privacy and personal data protection, a conceptual framework and hypotheses, and a summary of the chapter.

Chapter four justifies the methodology utilized to examine and explain the outcomes of the research questions. Also, this chapter discusses the research process and Literature analysis, including a systematic mapping study (SMS) on PPDP in the MCC and a systematic literature review (SLR) on determinants of preserving privacy and data protection. Moreover, this chapter presents the privacy by design framework, including the projected PbD framework in the high-level architecture of MCC and the projected framework and integration of hypotheses. Moreover, this chapter displays the data

collection and analyses, instrument, validity and reliability, SmartPLS, measurement model, and structural model. Lastly, the summary of the chapter is outlined.

Chapter five shows the result and discussion, including the result of data collection. Also, it presents the outcomes of the measurement model, including results of convergent validity and reliability, results of discriminant validity, and second-order. Moreover, this chapter offers the outcomes of the structural model, including coefficient of effect size (f^2), predictive relevance (Q^2), determination (R^2), the Goodness of Fit of the model (GoF), and hypotheses testing (Path Coefficient). Finally, a summary of the chapter is outlined.

Chapter six demonstrates the conclusion and future work, including a summary of principal findings, limitations, and research contributions. Finally, the conclusion and future research are given.

The references and appendix are included at the end of the thesis.

1.8 Summary of the Chapter

This chapter justifies the relevance of this research, where it presents and elaborates on the introduction, background, and motivation, including MCC, PPDP, and PbD. Moreover, this chapter shows the problem statement, research objectives, and research questions. It also presents the significance of the study and the thesis organization. The following chapter offers the related literature review.

CHAPTER 2: LITERATURE REVIEW

This chapter reviews the literature on MCC, privacy and personal data protection, current attacks and threats in MCC, privacy solutions projected to preserve PPDP in MCC, related work in information systems security and privacy, research gap of PPDP, and finally, the chapter summary.

2.1 Mobile Cloud Computing

This section presents MCC and the major actors in MCC. Also, it highlights the services of cloud computing and enterprise architecture and information systems security in mobile cloud computing.

2.1.1 Background of Mobile Cloud Computing

With the growth and spread of Cloud Computing (CC) and Mobile Computing (MC) as a new term, MCC has emerged since 2009 (Qi & Gani, 2012). To help us best understand MCC, let's begin with the two prior techniques: Cloud Computing (CC) and Mobile Computing (MC) (Qi & Gani, 2012).

2.1.1.1 Mobile computing

The mobility term has become prominent today, where it plays an increasingly significant role in the computing world. The growth of mobile devices like PDAs, smartphones, security technologies, laptops with a range of mobile computing (MC), GPS navigation, and networking has seen phenomenal growth (Qi & Gani, 2012). Moreover, with the advancement of wireless technologies such as WIFI, Ad Hoc Networks, and WiMax, users may enter the internet much more easily than previous, without being constrained by cables. Mobile users use various services provided by mobile apps, such as Google apps that operate locally on mobile devices or are offloaded to remote servers for execution (Momeni, 2015). As an outcome, a growing number of people have

accepted mobile devices as their primary mode of entertainment and communication in their daily lives (Qi & Gani, 2012).

Qi and Gani (2012) defined Mobile Computing (MC) as a type of human-computer interaction that a computer is supposed to transport with a regular operation (Qi & Gani, 2012). In addition, Somula and Sasikala (2018) defined mobile computing as a platform for information management that is not constrained by time or location. So, due to the platform's independence, users may access data from any location and at any time. As a result, irrespective of whether the user is stationary or mobile, the platform's functionality is unaffected (Somula & Sasikala, 2018). The three major concepts that make up mobile computing are software, communication, and hardware.

The concept of mobile computing hardware includes mobile devices like smartphones and laptops or their mobile components. Also, mobile computing software can be considered as mobile applications in mobile devices like mobile browsers, anti-virus software, and games. Mobile computing relates to powerful devices and handheld that allow mobility in wireless networks to support on-the-go computing (Bernsteiner et al., 2016).

Mobile devices have several issues with their resources, such as storage, bandwidth, battery life, communications, security, and mobility; therefore, quality of service is insufficient (Momeni, 2015). Since mobile devices lack processing power and storage, they cannot execute resource-intensive apps; hence, mobile users prefer to use more capable devices such as PCs and laptops to avoid resource scarcity issues (Momeni, 2015).

2.1.1.2 Cloud computing

Before the rise of Cloud Computing (CC), people suffered from storage space in the personal computer era. Users need high storage space and a high-performance operating system to keep pace with software development nowadays (Qi & Gani, 2012). Also,

centralized storage contains all the software applications, data, and services as part of Client/Server computing on the server-side (Nayyar, 2019). As a result, for a single person to access data, they need to gain access to the server. Besides, the concept of distributed computing was introduced, and resource sharing was made possible (Nayyar, 2019). Hence, the term CC emerged (Nayyar, 2019; Qi & Gani, 2012).

The term CC was first introduced in the 1950s when users accessed mainframe computers through dummy terminals in a central computer (Nayyar, 2019). Users did it to obtain access. Resource sharing was necessary because the prohibitively high costs of mainframes were not economically feasible. As a result, there was a crucial need to cut costs (Nayyar, 2019).

IBM, in the 1970s, released the virtual machine (VM) operating system, which enabled the use of many operating systems at the same time. VMs can permit Guest Operating systems to run on it, having their memory, infrastructure, and resource sharing also made possible. The concept of virtualization became very popular as a result of this development (Nayyar, 2019).

In the 1990s, telecom firms started offering virtualized private network connections that were more reliable and cost-effective than point-to-point services. As a result, companies are now able to give users shared access to a single infrastructure (Nayyar, 2019). Cloud computing evolution can be divided into three phases, which are as follows (Nayyar, 2019):

a) The idea phase began with the rise of service and grid computing in the early 1960s and lasted until the pre-internet era.
b) The pre-cloud phase began in 1999 and lasted until 2006. The internet was employed as the machinery for providing applications as a service in this case.
c) The cloud phase emerged in 2007, which includes the concepts of IaaS, PaaS, and SaaS that were explicitly defined and put into practice. Since then, cloud computing

has continued to evolve, altering end-user computing and changing the face of the world through resource sharing.

Since 2007, cloud computing has developed a common phrase among users. Though, there is no consistency in the definition of CC because dozens of organizations and developers termed it through their viewpoints (Qi & Gani, 2012). Hewitt (2008) stated that the primary aim of the CC system is to store data on cloud servers and use the temporary memory technologies for a customer to bring data where the customers could be using laptops, smartphones, personal computers, etc. (Qi & Gani, 2012). Moreover, as described by Buyya et al. (2008), CC is an equivalent and spread computing system that is made up of several virtual machines joined by internal links. Considering the Service Level Agreement (SLA), these systems dynamically deliver computing resources to clients from service providers (Buyya et al., 2008). Nevertheless, some authors referenced that CC was not a new concept as numerous existing concepts were only merged with some new ones in numerous research areas, such as networking service-oriented architectures (SOA), virtualization, and distributed computing.

The phrase "cloud" in relation to an Internet or network, means that the cloud is something available in a remote area where the cloud can provide benefits over the web or system, whether on private systems or open systems (Malik et al., 2018). Applications like online conferencing, email, and customer relationship management continue to operate in the cloud. CC relies on the computing of the web, which uses virtual shared servers to offer software infrastructure platform devices and other resources. Clients pay the host for the services as used services, where the digital system provides all data as a service in a CC model (Malik et al., 2018). In addition, cloud computing offers its clients many capabilities, such as access to an extensive number of users without the need to have a permit, shipping, purchasing, or downloading any of these applications. It also reduces the expenses of running and installing computers and software because no

infrastructure is required. Clients may access their data from any location using the system's interface (usually the internet). This means that cloud computing clients have many advantages, such as the ability to consume resources as a service and pay only for what they need (Malik et al., 2018).

There are three types of components for the cloud, presented as follows (Singh & Dhiman, 2021):

a) Clients: End clients utilize tools to manage their data in the cloud. Clients might be computer systems, navigation devices, tablets, mobile phones, and other smart devices.
b) Data Center: It is a physical location where businesses keep their critical apps and data. The design of a data center is built on a network of computing and storage resources that allow data delivery and shared applications.
c) Distributed servers: Additional computers are placed at regional locations to increase the availability and capacity. As a result, if one server fails to serve, the other can continue. Hence, clients are more versatile. When the cloud requires extra equipment, deploying new servers only in the data center is not essential. It is possible to connect them to another platform and only make them a part of the cloud.

Recently, cloud computing is becoming critical and getting great attention among users. Many users use document storage services such as Google Docs and Dropbox and social networking such as Twitter and Facebook (Nayyar, 2019). Also, they use photo storage sites such as Google Photos and webmail, where the only thing they all have in common is cloud computing services. In addition, Cloud computing is utilized by both large and small organizations as well as individuals. It ultimately comes down to the distant delivery of computing services over the Internet (Nayyar, 2019).

Cloud services are important to users in reducing the complexity and cost of having and running computers and other network resources. Some advantages include low

upfront costs, ease of customization, a quick return on investment, and rapid implementation (Nayyar, 2019).

2.1.2 Concept of Mobile Cloud Computing

Mobile Cloud Computing (MCC) as a concept has arisen out of two important trends: advances in mobile technology leading to ubiquitous mobile devices and cloud computing. According to Ratten (2017), MCC is an infrastructure whereby various mobile devices, for example, laptops, tablets, and smartphones, may access various computing resources at any time and from any location (Ratten, 2017). However, MCC raises ambivalence in terms of the opportunities it affords users. On the one hand, new mobile devices like smartphones deliver users with better accessibility and connectivity to applications and services (Ferreira & da Silva, 2014). Although mobile technology continues to evolve, the current terminals of mobile tend to suffer restrictions related to weak computational resources, for example, relatively slow processor speed, small disk capacity, and low memory size (Somula & Sasikala, 2018; Ferreira & da Silva, 2014). Storage capacity constraints on mobile devices led to migration to other storage services that provide storage needs, such as Google Drive, Box, iCloud, and Dropbox (Huang & Wu, 2017; JEEVAN et al., 2014). In addition to manually uploading data or files to the cloud, automated synchronization between the cloud and mobile devices is essential for mobile cloud storage services. Multimedia data created on mobile devices requires a stable and highly available storage solution. That's why many smartphones operating systems port multimedia data syncing capabilities (Google Drive for Android, SkyDrive for Windows Phone, iCloud for iOS, etc.) (JEEVAN et al., 2014). The majority of commercial cloud storage solutions are built-in centralized data centers suitable for the Internet and the cloud. On the other hand, CC delivers a strong approach to the provision of services by combining current technologies (Somula & Sasikala, 2018; Ferreira & da Silva, 2014).

The movement to MCC is eased by the improved association between the user providers and the technology providers that process efficiency and improve agility. MCC has two major advantages: services and technology. MCC enables more streamlined services with access to unlimited resources and collaboration. This is useful for moving processing and storage to cloud servers that can grip huge amounts of data. MCC uses the Internet, cloud, and computing in an elastic format accessible from multiple-geographic places (Ratten, 2017; Gai et al., 2016). Growing advancements in mobile communications mean more integrations with CC devices. The benefit of MCC is that it can ease technical difficulties that were earlier impossible without contact with high-performance computing services. New mobile cloud applications contain more energy-efficient storage and access to data (Ratten, 2017). The speed of wireless technology is critical for mobile users of CC services, for example, infrastructure and software. This is owing to an extraordinary rise in cloud computing services as the information economy expands (Ratten, 2017; Stantchev et al., 2015). As communication with online services has increased, there has been a desire to get data in mobile format. Moreover, CC technology has also been leveraged to hold over demand updates as consumer and business interactions for online purchases increase (Ratten, 2017).

2.1.2.1 The difference between mobile cloud computing and cloud computing

The difference between Could Computing (CC) and mobile cloud computing (MCC) is that CC specifically specializes in supplying virtual IT Infrastructure as a pay-as-go model, while MCC specifically offers cloud services to mobile devices (Shriwas et al., 2012).

2.1.2.2 Reasons of chosen mobile cloud computing in this research

Although significant research has been done on MCC (A Almusaylim & Jhanjhi, 2020; Alakbarov & Alakbarov, 2018), the researcher believes that there is a need for more studies in the field, such as this study for the following reasons:

a) Encouragement on the utilization of MCC for saving the personal data of the mobile user data due to the overall number of mobile devices that was predicted to hit 75 billion in 2020, with data volumes exceeding 24.3 exabytes (Malik et al., 2021). More significantly, research reported the right to PPDP in the age of new technologies (Kucharczyk & Joachymczyk, 2021).
b) Expansion of the researcher's knowledge of MCC, including PPDP in the MCC.
c) An attempt to improve features provided by MCC by including novel features such as select storage location, which is classified based on the application of laws and regulations.

2.1.3 Enterprise Architecture and Information Systems Security in Mobile Cloud Computing

It is stimulating to note that mobile cloud computing saves mobile resources (including applications and data from external providers) on mobile devices (Somula & Sasikala, 2018; Fernando et al., 2013). For instance, users can store private personal life stories, private family information, and personal data. Also, private business data and information can be stored in the cloud. Overall, the user may access his data irrespective of their present location. In summary, MCC is a field that comes from the advancement of cloud computing and mobile technology. MCC offers virtually unlimited dynamic resources for computation, service provision, and storage (Somula & Sasikala, 2018; Fernando et al., 2013).

As shown in Figure 2.1, the MCC architecture provides a model that incorporates the features of cloud computing and mobile technology. Figure 2.1 demonstrates that mobile users may use mobile devices such as PDAs, smartphones, and tablets connected to the network through station satellites or base transceivers (BTS) (Hanen et al., 2016).

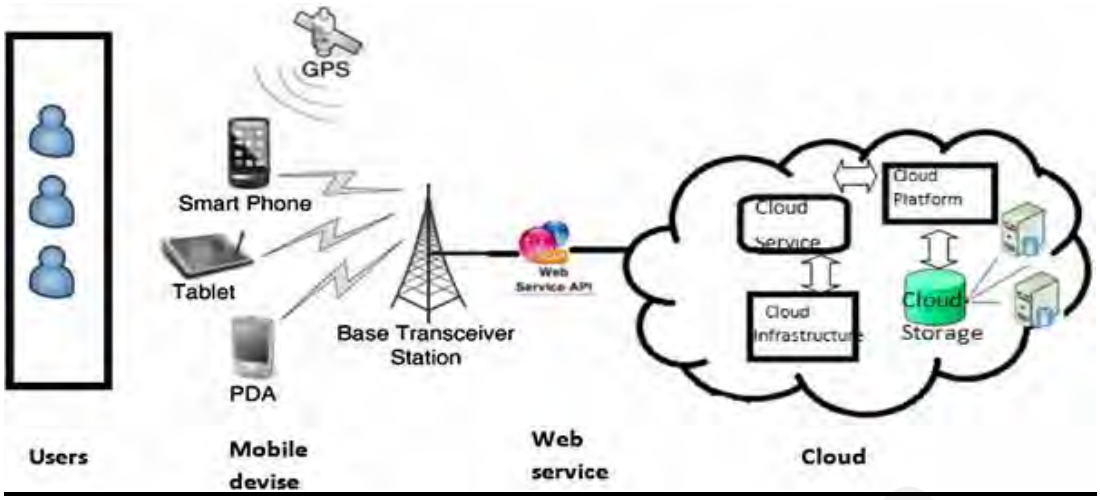


Figure 2.1: Enterprise architecture of MCC (Hanen et al., 2016)

As shown in Figure 2.1, the needs of the users of mobile are broadcast to the servers that provide services of mobile, and then subscribers' needs are dispersed to the cloud services. Lastly, the cloud controller sends to the users with the desired cloud service (Hanen et al., 2016).

Research in enterprise architecture and information systems security in MCC continues to enhance privacy and personal data protection, and articles are published in the domain, such as supporting compliance with the General Data Protection Regulation (Burmeister et al., 2019). The current study is considered to be in the domain (Enterprise architecture: information systems security in mobile cloud computing), where this research demonstrates the PbD framework for privacy and personal data protection in MCC.

2.1.4 High-Level Architecture of Mobile Cloud Computing

From the concept of MCC, the user stores their data in the cloud, the processing is run in the cloud, and the mobile devices serve as display media. In the high-level architecture, the MCC provides a model that incorporates the features of cloud computing and mobile technology (Hanen et al., 2016). Figure 2.2 illustrates the high-level architecture of MCC that includes registration, mobile cloud computing storage service, and synchronization. In other words, this high-level architecture consists of two phases, including registration

and synchronization (Faheem et al., 2016; Gothawal et al., 2015). More importantly, this high-level architecture reflects the whole architecture of the MCC, where the mobile cloud computing user can register and use the cloud service using their mobile device. The phases are presented as follows:

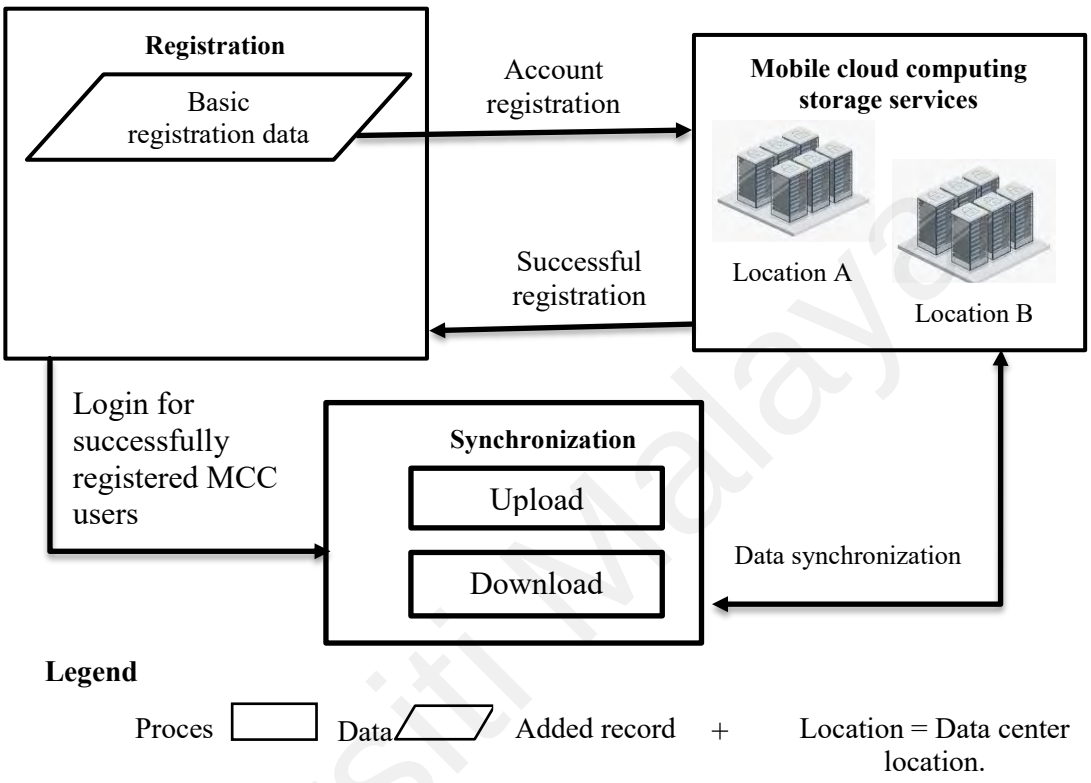


Figure 2.2: High-level architecture of MCC

Phase A: Registration: In Phase A, the mobile cloud computing user have to register to use the mobile cloud computing storage.

Phase B: Synchronization: As presented in the literature, the mobile cloud computing storage service synchronizes with the available storage services (Flores et al., 2011). Personal data saved on the mobile device is synchronized with the server, leading to a mobile cloud computing storage service during the synchronization phase. The updated, deleted, or added data is reflected automatically in the storage through download and upload (Cui et al., 2017).

2.1.5 Major Actors in Mobile Cloud Computing

There are five principal participants in cloud computing based on their engagement. A cloud service consumer (CSC) or cloud consumer is the client who pays for the service as per the use to have the service from a cloud provider (for example, Google Drive users). The cloud service provider (CSP) or loud provider is a provider that offers cloud services to cloud service consumers (for example, Google Cloud). A cloud auditor is the one who conducts an independent valuation of the security of the cloud implementations, cloud services, performance, and information system operations (Like HIPAA in healthcare). A cloud broker is the one who consults, mediates, and cooperates with CSC and CSP to facilitate the selection of cloud computing solutions and make the business happen (for example, Appirio or AWS Marketplace). The cloud carrier is the one who delivers cloud services and connectivity from cloud service provider to cloud service consumer (ex., Telecom carriers or a transport agent like Maxis communications in Malaysia) (Kumar et al., 2018).

2.1.6 Services of Cloud Computing

Three models of service distribution seem to represent the majority of deployments: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-service (IaaS). Some features that make cloud computing a compelling choice include:

a) Rapid elasticity: The distribution of resources is flexible and fast provisioned based on the customer's requirements, where they can purchase unlimited resources based on their demands at any time, which means that the system needs to be elastic enough to meet the needs for increasing demand and return to the normal levels when demand decreases (Haque et al., 2020; Amini & Jamil, 2018).

b) On-demand self-service: Cloud services are available at all times; it is platform-independent and often accessed through a web service API or a web browser without passing via a specific service provider. In other words, the user can manage and

request the need of the service when they want and pay (pay-and-go) without any action of a human with a CSP (Haque et al., 2020).

c) Measured Service: Service charges are determined by consumption (pay as you use) (Haque et al., 2020).

d) Resource pooling: Computing resources are merged to serve several clients using various virtual and physical resources that are dynamically allocated and reassigned based on requests (Amini & Jamil, 2018).

e) Broad Network Access: The resource availability and user information in many virtual machines generate a dynamic collection of resources that could be affected by unauthorized access (Amini & Jamil, 2018).

In the IaaS, the cloud service provider only offers infrastructure such as storage, server, networks, and virtualization. The cloud service consumer is accountable for operating systems, runtime, applications, data, and middleware. Also, in PaaS, only the data and application are cloud service consumers' responsibility, and the rest of the services are delivered by cloud service providers. In SaaS, all the services are offered by cloud service providers (Kumar et al., 2018). Security issues are also affected by cloud deployment models. These features are available in the various models of deployment: community cloud models, hybrid cloud, public cloud, and private cloud.

2.2 Existing Attacks and Threats in Mobile Cloud Computing

In this thesis, a systemic mapping was conducted on PPDP in the MCC. A systematic mapping study was conducted, where 1711 papers published from the year 2009 to the year 2019 were initially collected, followed by a filtering process; as a result, seventy-four primary studies were selected and investigated where the existing data privacy attacks and threats in MCC were identified.

As shown in Table 2.1, in the search result, 215 studies were obtained. Correspondingly, 128 studies were comprehensively analyzed. After the screening

process, only seventy-four primary studies were chosen for SMS. Further, the detailed study of the SMS is presented in detail in sub-section 4.2.1, under the chapter research methodology.

Table 2.1: The results of the process of filtering the studies

Results / Database	Search result	Comprehensive analysis	Final selection
Science Direct	78	37	31
IEEE Xplore	47	27	20
Scopus	65	46	16
ACM	9	5	4
Springer link	16	13	3
Total	**215**	**128**	**74**

The result of the SMS identified attacks and threats in MCC. Based on the number of research, Figure 2.3 shows the proportion of primary studies connected to attacks and threats. As shown in Figure 2.3, the most popular attacks and threats are unauthorized attacks and threats with 18%. Followed by data privacy, leakage of user privacy, data misuse, and untrusted service provider with 15%, 13%, 11%, and 11%, respectively. Conversely, disclosing the information or the data, and man-in-the-middle attacks are having 6% and 5%, respectively.

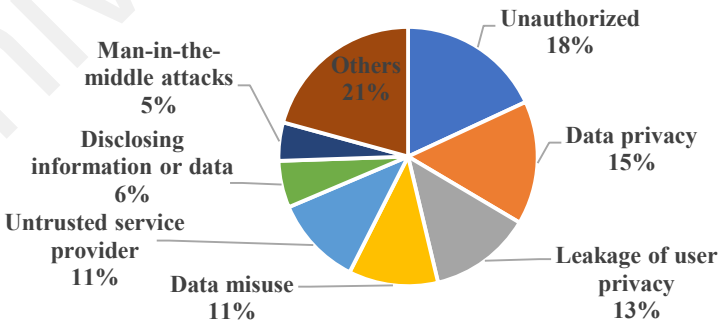


Figure 2.3: Attacks and threats

For clarification of some of the mentioned threats and attacks in Figure 2.3, unauthorized access refers to a person acquiring physical or logical access without authorization to a system, network, data, application, or another resource (Sindhu &

Meshram, 2012). Data privacy is defined as one of the fields of data protection concerned with the proper processing of data that emphasizes compliance with data protection regulations (Riyadi, 2021). Disclosing information refers to the sensitive information released to others intentionally or unintentionally (Dodiya & Singh).

Furthermore, Figure 2.4 is a Bubble-plot of attacks and threats, the Y-axis displays the attacks and threats, and the X-axis displays the years. The outcome of the study illustrates that improper security practices and policies in some locations, leakage of user privacy, phishing attacks, and unauthorized data privacy are quite dominant in the domain. Conversely, inference attacks on user privacy, internal attacks, eavesdropping attacks, data breach threats, and internal multi-layer attacks are losing motion.

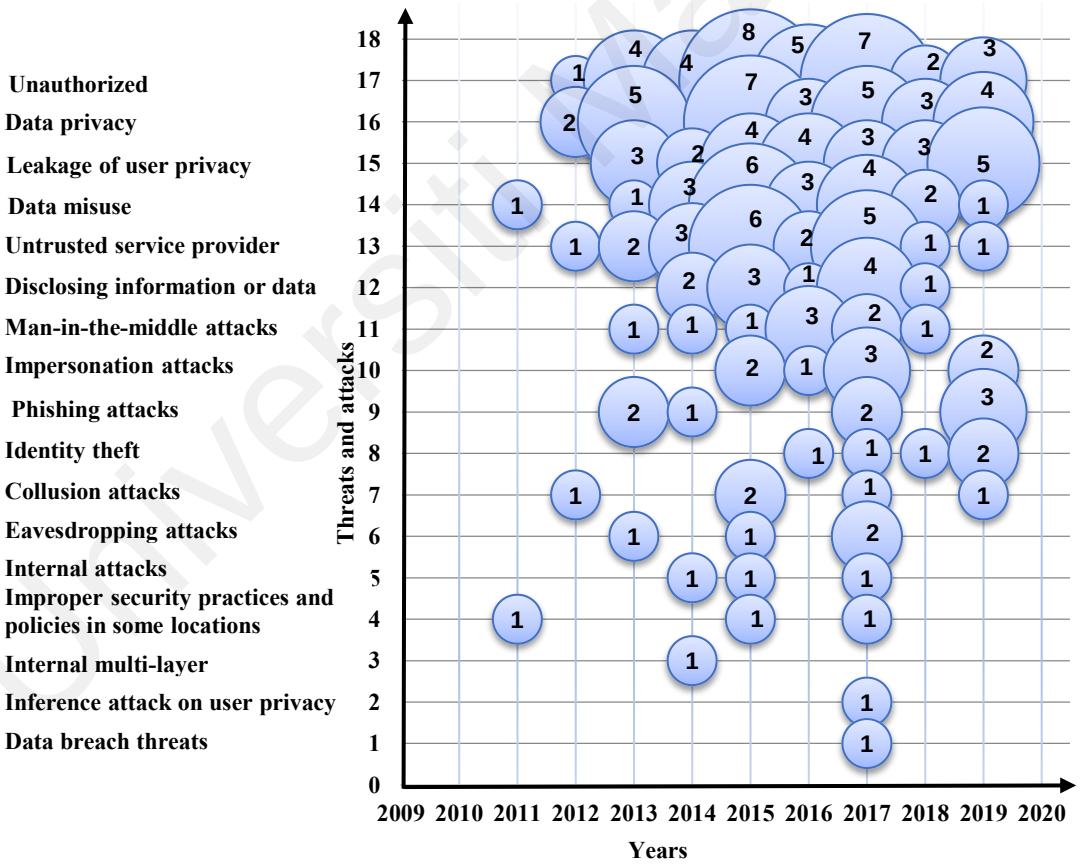


Figure 2.4: Bubble-plot of attacks and threats

2.2.1 Issues Related to Privacy and Personal Data Protection in MCC

The issue of privacy and personal data protection (PPDP) in mobile cloud computing may cause threats and attacks such as:

a) A personal data breach: is defined as a security breach that results in unintentional modification, loss, illegal destruction, unauthorized disclosure, or access to personal data that has been stored, sent, or otherwise used (Organization, 2021).
b) Data misuse: in general, the use of information is controlled by policies, agreements, laws, and regulations, and data misuse happens when such data is utilized outside the scope of these laws. For instance, copying organizational sensitive information to personal devices makes it available for others to view and steal it (Odusote, 2021).
c) Identity theft occurs when somebody steals someone's personal or financial identity. The identity thief may be utilizing the information to either earn something like money or to injure another person's reputation (Zukarnain, 2021).
d) Disclosing personal information refers to the sharing or disclosing of personal information to others without authorization from the owner to do so (Maurushat, 2019; Harfoushi, 2017).
e) Private information leakage occurs when a system releases a user's private information to an entity that is not authorized to have access to this data; such leaking often happens without the user's authorization (Landau et al., 2020).
f) Others: Mobile cloud computing users might unwillingly be exposed, for example, social trolling and shaming, spying, internet viruses, stealing user information, and spam messages (Qayyum, 2020; Maurushat, 2019; Burgess, 2013).

An important question is how does the location of cloud storage affect MCC?. To answer this question, research reported that data on the cloud could be kept in multiple sites across countries, which can be protected in one country and not protected in another one (Baharon et al., 2015). Furthermore, the nature of the cloud has significant consequences on personal data privacy, counting questions about who has access to it and how to secure the location (Baharon et al., 2015; Angin et al., 2010), which might impact the decision of MCC to use cloud storage (Angin et al., 2010). Moreover, studies noted

that improper security practices and policies in some locations are among the issues of PPDP in mobile cloud computing (Qayyum, 2020; Vatka, 2019; Baharon et al., 2015; Li et al., 2015; Huang et al., 2011).

2.3 Privacy Solutions Proposed to Preserve Personal Data Protection in Mobile Cloud Computing

In this thesis, a systemic mapping was conducted in PPDP in the MCC. A systemic mapping study was conducted, where 1711 papers published from the year 2009 to the year 2019 were initially collected, followed by a process of filtering. Finally, 74 primary studies were selected and investigated. However, current privacy solutions projected to preserve PPDP in the MCC were observed. For more clarification about the systematic mapping study, Sub-section 4.2.1 in the research methodology demonstrate the method.

Based on conducted SMS, Figure 2.5 is a Bubble-plot of the existing privacy solutions. Y-axis demonstrates data privacy solutions, and the X-axis demonstrates the years. The outcome in Figure 2.5 defines that the research is growing concerning encryption and authentication data privacy, and there are few studies on trust. Based on the result, privacy by design is not utilized as a solution in the domain. As a result, this study attempts to utilize privacy by design as a solution in the domain.

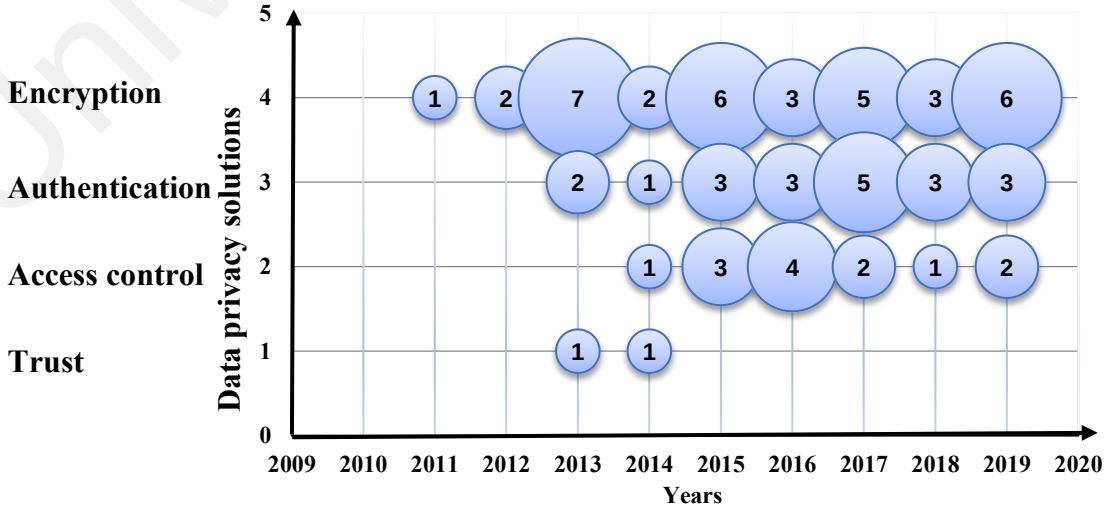


Figure 2.5: Bubble plot of privacy solutions

Figure 2.6 displays the percentage of research associated with privacy solutions. The result illustrates that the studies concentrated on encryption with 50%, authentication with 28%, and access control with 19 %. The results show that two research offered trust solutions, indicating that new solutions are looming in the domain.

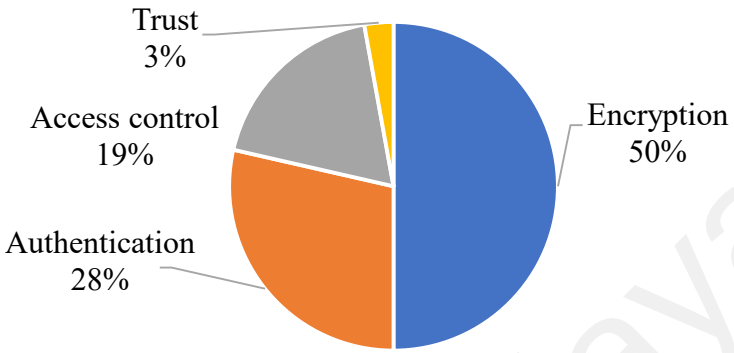


Figure 2.6: Privacy solutions

2.4 Privacy and Personal Data Protection (PPDP)

This section demonstrates the concept of data privacy, privacy laws, and personal data.

2.4.1 Data Privacy

The Internet creates a privacy nightmare because people disclose their personal information, whether intentionally or not. When people buy food, receive medical care, pay taxes, listen to music, communicate with family members, and participate in social media, they provide organizations with a wealth of personal data and information (Garlie, 2020). Organizations that gather personal information from individuals announce their intention to collect, preserve, and share the privacy policy of their websites. Unfortunately, individual privacy policies are often difficult to understand, where sometimes there is vague information that can only be understood by lawyers (Garlie, 2020). The users are led into a false feeling of security by the availability of privacy policies. Pew Research Center conducted a survey where a majority of the respondents thought that these policies describe the way of keeping personal data confidentially by the organization, not knowing that they are only protecting themselves (Garlie, 2020).

Allen (2013) claimed that this is an era of "the great information privacy give-away" and that people today are giving away more personal information to strangers than ever before (Garlie, 2020). Moreover, Amazon, Facebook, Google, Match.com, Microsoft, and Twitter use systems to enhance the user experience, for example, finding lost friends on Facebook and discovering new movies similar to ones that others enjoyed and ranked on Netflix through their black box (Garlie, 2020). Over time, technology has evolved where home automation devices record conversations (Garlie, 2020). In addition, Smartwatches alert their users when they meet their daily step targets of 10,000 steps, where it is easy for the provider to capture and analyze their geolocations (Garlie, 2020).

Although Allen (2013) claimed that commentators and scholars admire and support those who freely share personal details in the give-away since it benefits society, however, he argued that this give-away is risky and unethical due to the potential outcomes of reckless behavior (Garlie, 2020). Moreover, the paradigm shift towards sharing has spread an inattention to the appropriate protection of personal data because of reckless behavior in surrendering personal data (Garlie, 2020; Mai, 2016). For example, the researcher presented a case of one who willingly shared images through Twitter, and he faced legal consequences due to this reckless behavior (Garlie, 2020). Furthermore, Allen suggested that governments and corporations should be shared in the obligation to protect personal data (Garlie, 2020).

The concept of privacy varies greatly in different jurisdictions, cultures, or countries. The Organization for Economic Cooperation and Development (OECD) (Co-operation & Development, 2002) defines privacy as any information concerning a recognized or identified person (data subject) (Alguliyev et al., 2019). In general terms, privacy is associated with the storage, destruction, collection, disclosure, and use of personal data (or personally identifiable information (PII)) (Alguliyev et al., 2019; Accountants & Accountants, 2009).

Privacy is the capability of a group or an individual to isolate themselves or their data and thus talk about themselves selectively. Privacy in CC is evident as the capability of a business or a user to observe what data they disclose about themselves over the cloud (or to a cloud service provider) and the capacity to manage who has access to that data (Ranchal et al., 2010).

Confidentiality of information refers to the right of an individual to control personal data about himself or herself, the right to withhold such information, and to prevent others from accessing it (Cassidy, 2018). In addition, data privacy is concerned with the use, collection, processing, distribution, and transmission of personal data generated in our daily lives (Cassidy, 2018).

Privacy plays a critical role in guaranteeing the protection of human rights, as it is an important fundamental element of human freedom; where it is difficult to deny this fact and ignore the fact of privacy for what it contributes to the increase of personal freedom of the individual (Mantelero, 2016). Therefore, the protection of personal information is a requirement for everyone, which will affect everyone like friends, co-workers, family, relatives, and many others if the protection of personal data is ignored (Grundstrom et al., 2019; Commission, 2010). To be exact, privacy is more than simply concealing information, it is an authentic control over personal data with the consideration that no one has the right to receive personal information without the owner's consent unless there are regulations that enable such access (Kayaalp, 2018), for instance, income data that the authorities may obtain. According to previous studies, identifying private data implies particular application consequences, in which laws and regulations are keys to personal data protection (Bansal et al., 2016; Chen & Zhao, 2012).

Nowadays, privacy in mobile cloud computing has gained more attention; though various current privacy regulations and laws are required to impose principles for the usage, disclosure, maintenance, and collection of personal data, which must be fulfilled

even for cloud service providers (Gellman, 2012). Also, research stated that there is an increased risk of privacy when locating your information in someone else's hands (Gellman, 2012).

The ownership and administration of a user's data are handled by separate persons, where the user owns it and the cloud provider manages it. This may force some users to reconsider their data storage in MCC, lowering MCC's popularity (Rayapuri, 2018). Another issue is that user data is also stored on shared infrastructure, which can be stored in an unknown location anywhere in the globe, and cloud providers will not disclose the location of user data to users. These two issues raise the danger of user data being exposed. Therefore, a permanent solution is needed to protect sensitive data and maintain secure privacy (Rayapuri, 2018).

2.4.2 Privacy Laws

The investigations have reported that many current privacy laws force maintenance criteria, use, collection, and expose personal data, which would have even been complied with the cloud provider (Ranchal et al., 2010; Gellman, 2009). Consequently, like CC, there is little, or occasionally no data accessibility in the cloud to indicate where information or data is stored, how safe it is, who has access to it, and whether it is conveyed to another host, or if the host can be trusted (Angin et al., 2010). Research reported that information in the cloud might affect the confidentiality and privacy of data and that of those responsible for storing or handling data (Ranchal et al., 2010; Gellman, 2009).

Moreover, when users use programs residing on someone's hardware to store their data, they usually miss some control over their confidential information (Shen et al., 2018). The responsibility of guarding that information against hacker attackers and internal data breaches rests with the hosting company rather than individual users (Mollah et al., 2017). Government investigators seek to subpoena information that could approach

that firms without telling or consenting the data owners. Some businesses may even voluntarily share sensitive data with marketing companies (Ranchal et al., 2010). So, when your data is in other people's hands, privacy risks will always increase (Venkatesh & Eastaff, 2018; Ranchal et al., 2010).

Studies reported that privacy law is the law that deals with storing, regulating, and using personally identifiable information of individuals, which can be collected by public or private organizations, governments, or by other individuals (Mulligan et al., 2019; Ranchal et al., 2010).

For complying with global privacy regulations, organizations should guarantee the protection of the information saved on their cloud providers by implementing both technical controls and managerial. This is particularly critical and important for organizations dealing with global data (Deloitte, 2016).

In summary, to reach the best practical effect, the organizations should actively manage the legal agreements. Notably, the organizations must require frequent updates on the effectiveness of their providers' security and privacy measures, as well as their database activities, together with the revelation of any issues or incidents that may put information in danger (De Filippi & McCarthy, 2012).

2.4.3 Personal Data Protection

Personal data refer to any form of data having to an identified or identifiable individual (Data Subject); an identifiable individual can be recognized, indirectly or straight, particularly by orientation to a personal identification number or through one or more aspects particular to his physiological, economic, physical, mental, social identity or cultural. Examples of sensitive personal data are religious beliefs, membership of details of sexual life, trade unions, mental health and physical, racial and ethnic origin, and politics (Grundstrom et al., 2019; consulting, 2018; Wong, 2007). Also, personal data is known as personally identifiable information (PII) or personal information (Lah, 2008).

According to Skendžić et al. (2018), personal data protection is a right to the protection of legitimate rights of an individual, which includes prevention of and punishing personal data misuse, and it is safeguarded by international and national legislation. Also, according to the same authors, the individual (data subject) means is any natural individual who may be recognized straight or indirectly, in specific by orientation to an identifier, for example, a location data, email, address, name, or through factors specific to the person's mental health or condition, physical health or condition, social identity or cultural, political views, religious or other similar beliefs, economic, criminal records (Skendžić et al., 2018). Therefore, those data are highly confidential, and it is important to enforce privacy and protect this personal data in MCC.

Additionally, recent consideration towards privacy issues, including policymakers, companies, and users showing risks, including blackmailing, information breach, collection of private information, and social engineering (Hayes & Cappa, 2018). Moreover, efforts have been made to solve privacy issues and personal data protection. For instance, in Europe, regulations, and laws on data collection and exposure are established through General Data Protection Regulation (GDPR) (Dove, 2018; Alnemr et al., 2016; Pearson, 2013).

In privacy law and data protection, including the GDPR, its definition goes beyond the general use of the phrase “personal data," which can, in reality, be applied to numerous sorts of information that help in recognizing or finding a natural person in the area of the GDPR. For example, it contains information that can be used for an individual's straight or indirect identification. The GDPR governs the handling of personal data. This means that the GDPR has established rules for protecting personal data, aimed at protecting the privacy and fundamental rights of European citizens (Purtova, 2018; i-scoop, 2016).

When you read the personal data for GDPR definition in Article 4 (1), it consists of several elements such as “Any Information, Relating to, Natural person, and GDPR data subject: identified and identifiable” (consulting, 2018).

a) Any information: Overall, from the GDPR perspective, any information should be understood accurately, which can be a name or biometric element used for identity verification. For example, the fingerprint or facial recognition, a cookie (one of the forms of online identifiers), an email address, a person's location, a health-related data element, gender, occupation, physical factor, and indeed anything (Purtova, 2018; i-scoop, 2016).
b) Relating to: In fact, the information relates to somebody, and this information may affect the privacy right of the person to whom the data refers.
c) Understanding the contextual aspects is important for General Data Protection Regulation to make it accessible. Think of a basic Excel sheet or database with only a set of first names. If it is not suitable in a larger context or can be tracked about someone then the list does not include any personal information but only the name. For example, one can use them to create a list of the most common first names that are fully anonymous (Purtova, 2018; i-scoop, 2016). However, when further context is provided in the form of information such as the person's surname and job function, All of the information pieces, including the first name, become personal (Purtova).
d) Natural person and General Data Protection Regulation data subject (identified and identifiable): Basically, a normal individual means everyone, such as me, you, and all of us. The GDPR applies within the geographic scope known by the GDPR to only “real people, which means the business is not a natural person. In the manuscript, the natural persons to whom the data subjects are “any information relates to”. Now adding additional elements is needed, mentioning to normal persons where the data subjects are if they are identified or identifiable (Purtova, 2018; i-scoop, 2016).

2.5 Related Work in Information Systems Security and Privacy

Several studies investigated data issues (Koloseni et al., 2019; Dodel & Mesch, 2017; Schymik & Du, 2017; Ameme & Yeboah-Boateng, 2016; Humaidi & Balakrishnan, 2015; Williams et al., 2014; Humaidi & Balakrishnan, 2012; Claar & Johnson, 2010; Ng et al., 2009) related to this studies found in the literature. For instance, Ng et al. (2009) utilized the HBM to explore users' computer security behavior. They collected survey data from 134 employees. However, the outcomes of the research illustrated that the perceived susceptibility and benefits are the constructs of email-related security behavior (Ng et al., 2009). Another study projected a conceptual framework that utilized HBM to interpret why nearly people are not conscious of threats that is adequate to prompt computer security software adoption (Claar & Johnson, 2010). Moreover, Humaidi & Balakrishnan used surveys, questionnaires, along with interviews to measure the effect of security technology and awareness on the behavior of the users toward health information system security based on PMT and HBM (Humaidi & Balakrishnan, 2012). They discovered the modest effect of the health professional's experience on the relationship among factors of the Health Information System Security Policies Compliance Behavior (HISSPC) model (Humaidi & Balakrishnan, 2015). The proposed model has been verified via the PLS and the results point to R^2. Also, Williams et al. established a model called the security belief model, which is constructed from the current health behavior model (Williams et al., 2014), The model was tested empirically and evaluated on a sample of 237 professionals. The outcome pointed to the overall support for the established model, particularly severity, susceptibility, cue to action, and as benefits antecedents to the intention to perform preventive information security behaviors (Williams et al., 2014). In addition, Dodel & Mesch (2017) provided a cyber-victimization preventive behavior using the health belief model. They presented a model on factors of a non-digital preventive (Dodel & Mesch, 2017). They also studied the factors of cyber-safety,

particularly factors associated with the usage of the anti-virus on Internet networks. The outcome of the study showed the role of attitudes and values in the decrease of threats. Furthermore, Koloseni et al. used the health belief model to study employees' security behaviors, particularly both automatic or habitual security behaviors and conscious security behaviors of Tanzanian government employees (Koloseni et al., 2019). The research outcome supported that cues to the action, perceived barriers, perceived severity, security habits, and perceived susceptibility affected the intentions of government employees in practicing information security behavior (Koloseni et al., 2019).

Additionally, another research seeks to define the email security behaviors of undergraduate students (Schymik & Du, 2017). A survey was used and based on the health belief model; a questionnaire was established. The investigation suggested that perceived benefits affect students' security behavior (Schymik & Du, 2017). Moreover, a recent study attempted to clarify the motive for security breaches and established a model that utilizes the health belief model to predict internet banking customers' behaviors (Ameme & Yeboah-Boateng, 2016). The authors noted a relationship between customer behaviors and internet banking security breaches. Interestingly, the authors claimed that their findings have important policy implications for banks, allowing them to better understand customers' behavior on internet banking (Ameme & Yeboah-Boateng, 2016).

2.6 Research Gap of Privacy and Personal Data Protection in MCC

Recently, the demand for information security has been increasing because of data breach cases worldwide (A. A. Ikram et al., 2021; Asrani, 2013). So, the protection and privacy of mobile cloud computing data are being widely acknowledged as a key security issue (Nawrocki et al., 2022; Ryan, 2011). However, despite the seemingly appropriate MCC nature, it presents several users with challenges regarding the security of their data (Anjaneya et al., 2021; Chaubey & Tank, 2016).

The emergence of mobile cloud computing raises an extensive range of useful services that assist in several aspects of human life (AlAhmad et al., 2021; Le Vinh, 2017). However, there are many issues regarding the location of cloud storage in which user's data is hosted (Venkatesh & Eastaff, 2018; Zhou & Huang, 2012). In addition, given the fact that the world has become a global village, these entities are at liberty to set up servers in any country and store user information without informing the client (Mollah et al., 2017; Khan et al., 2013). By doing this, they disregard various vital features such as the predisposition of this country to user data privacy, laws and regulations for cloud computing, and the relationship with the source country (Akhtar et al., 2021; Vaile et al., 2013; Wang, 2011).

Based on the result of the SMS, as shown in Figure 2.4, data privacy, unauthorized access, phishing attacks, and leakage of user privacy are relatively dominant. The result of SMS also shows that there is a lack of research on improper security practices and policies in some locations, internal attacks, data breach threats, inference attacks on user privacy, eavesdropping attacks, and internal multi-layer attacks. As shown in Figure 2.4, a few studies focused on the improper security practices and policies in some locations and this study has considered this gap.

Based on conducted SMS, as shown in Figure 2.5, four solutions were presented to preserve privacy in the MCC in chosen primary studies, including access control, authentication, trust, and encryption. Based on the result, privacy by design is not utilized as a solution in the domain and as a result, this study attempts to utilize privacy by design as a solution in the domain.

In summary, the nature of the CC has an important effect on the privacy of personal data, including concerns about who has access to it and how secure the location is (A Almusaylim & Jhanjhi, 2020; Angin et al., 2010), which affects the mobile cloud computing user's decision for using cloud storage (Qayyum, 2020; Angin et al., 2010).

Although debate continues over the best strategies for dealing with the different issues of PPDP in mobile cloud computing, to the best of the researcher's knowledge and based on the SMS result, the benefits of utilizing privacy by design (PbD) to preserve PPDP in mobile cloud computing are not investigated. PbD is used in this study since privacy protection should be addressed across the product life cycle, from the beginning till the end (Bu et al., 2020; Cavoukian, 2009).

2.7 Privacy by Design

Privacy by design (PbD) was reported by a combined team of the Information and Privacy Commissioner of Ontario, the Dutch Data Protection Authority, and Canada to examine the foundation of PbD in 1995. Through this collaboration, they published a study on "Privacy Enhancing Technologies" (Bu et al., 2020; Hustinx, 2010). The concept highlights active protection and states that privacy should be handled throughout the product's life cycle, from the beginning to the end of its useful life (Bu et al., 2020; Cavoukian, 2009). PbD is a novel privacy protection concept that can deliver broader protection of privacy information (Bu et al., 2020). In 2008, Cavoukian proposed the seven basic principles of PbD, providing a framework for understanding and implementing PbD (Cavoukian, 2009). The principles established that the protection of private data should be preventive rather than corrective; privacy must be included in the design; it should be considered as a default rule; PbD goals can achieve all legitimate interests in a win-win way. At the same time, privacy protection should be enabled during the product data-related life cycle, and privacy-related behaviors should be visible and transparent to vendors and users. In summary, the primary concept of privacy by design is to preserve users' privacy (Bu et al., 2020; Cavoukian et al., 2010).

Over the past decade, the concept of PbD has grown and been widely disseminated as a conceptual model for the protection of personal data. Moreover, in the year 2010, privacy by design was formally acknowledged during the 32nd International Conference

of Data Protection and Privacy Commissioners as an “essential component of fundamental privacy protection” and recommended by organizations, making PbD Foundational Principles a section of their default operation (Bu et al., 2020; Cavoukian & Chibba, 2018). Later, PbD has been widely included in privacy protection laws and businesses in a variety of nations. The US Federal Trade Commission in the year 2012 recommended that PbD should be considered the preferred method of improving security and privacy online. Moreover, in the same 2012 data protection directive, the European Union Council recommended PbD (Cavoukian & Chibba, 2018). In 2015, the United States proposed the Corporate Privacy Rights Act, where PbD was recommended as a business practice (Bu et al., 2020). In addition, privacy by design is quickly developing and has become a documented privacy framework in the data industry, which is being debated in different domains such as healthcare systems, big data, biometric encryption, the internet of things, etc. (Bu et al., 2020; Cavoukian & Chibba, 2018; Cavoukian et al., 2010).

Privacy by design is a technique of system engineering that thinks about privacy from the beginning to the end of the full engineering process (Bernsmed, 2016). This notion has fast expanded in two main areas, including architectural design and information management (Schaale, 2014). The first of them concentrate on constructing the correct architectures in web systems and data centers with an emphasis on submitting to actual regulatory environments and even including tools and processes to decrease clients' privacy concerns. The other one belongs to applying accumulation, control, and de-identification mechanisms and operations to manage analytics and big data collection while taking into account privacy and sovereignty limitations or adjustments (Schaale, 2014), where PbD is a philosophy that enables software developers to use embedded ways to protect users' privacy (Hadar et al., 2018).

"The general philosophy of PbD is that privacy should not be treated as an afterthought but rather as a first-class requirement during the design of a system" (Morales-Trujillo et al., 2018). In other words, while defining the architecture and features of a system, designers should consider privacy from the outset (Cavoukian, 2020; Hadar et al., 2018; Le Métayer, 2010).

Privacy by design is considered an active protection paradigm that can provide greater privacy protection over the whole lifecycle of information products (Bu et al., 2020). Interestingly, it is becoming the main pattern for privacy protection (Bu et al., 2020). It is considered a potential development trend in the data industry, where it is gaining the concern of practitioners and researchers (Bu et al., 2020).

Privacy by design is the action mandated by the companies, especially the cloud computing providers, to ensure activities on a person's data are escorted by the provision of security and privacy. Privacy by design is established in the 1990s (Pagallo, 2021; Bu et al., 2020). It has gradually distilled by Cavoukian and founded upon seven fundamental principles as follows (Bu et al., 2020; Cavoukian, 2010; Langheinrich, 2001):

a) Proactive, not Reactive; Preventive not Remedial: The first fundamental principle illustrates that data privacy must be thought of from the setup of the data security planning process, not after a data breach (Bender et al., 2017; Bernsmed, 2016; Cavoukian, 2010).
b) Privacy by default: The second fundamental principle is that privacy by default aims to provide the highest level of privacy possible by guaranteeing that personal data is automatically safeguarded in any IT system or business practice (Bender et al., 2017; Cavoukian, 2010).
c) Privacy embedded into the design: The third fundamental principle means that the privacy embedded in the design is not an afterthought but rather an integral

component of the primary service being offered (Bender et al., 2017; Cavoukian, 2010).

d) Privacy by positive-sum, not zero-sum: The fourth fundamental principle means that there should be neither trade-offs nor false dichotomies of privacy. One may have revenue, expansion, and privacy without compromising one for the other (Bender et al., 2017; Cavoukian, 2010).

e) An end-to-end security-full lifecycle protection: The fifth fundamental principle reports that end-to-end security-full life cycle protection is a cradle-to-grave life cycle control of information, end-to-end which in the privacy protections follow the data since its creation, sharing with others, and eventually archiving (Bender et al., 2017; Langheinrich, 2001).

f) Visibility and transparency: Keep it Open. Privacy by design is intended to convince all concerned sides that whatever the business practices or technologies concerned, it is, in fact, subject to independent verification, operating according to the promises and objectives stated. Its constituent parts and process remain visible and transparent to both providers and users being the same however, keep in mind, trust but verify (Bender et al., 2017; Bernsmed, 2016; Langheinrich, 2001).

g) Respect for user privacy: The final fundamental principle is respect for user privacy, which clarifies the data owned by the customers. The data kept by an organization must be accurate, and the customer must be given the ability to make adjustments. The customer is also the only one who has the authority to provide and revoke consent for the use of data (Bender et al., 2017; Langheinrich, 2001).

In the PbD research domain, investigating one of the PbD principles and generalizing the outcomes is a common practice (Ehécatl Morales-Trujillo et al., 2019; Cavoukian, 2017, 2010; Cavoukian & Spencer, 2010). Furthermore, a recent SMS has discovered that many research in privacy by design studied at least one privacy by design principle and

generalized the outcomes (Ehécatl Morales-Trujillo et al., 2019). Prior studies have shown that privacy by design is established upon 7 fundamental principles, which are determined by Cavoukian (Bender et al., 2017; Kroener & Wright, 2014).

2.8 Summary

This chapter illustrates a comprehensive literature review consisting of the MCC, privacy and personal data protection, existing attacks and threats in mobile cloud computing, and the current privacy solutions proposed to preserve personal data protection in the MCC. Also, to achieve RO 1, an SMS study was conducted, where 1711 papers published from the year 2009 to the year 2019 were initially collected, followed by a process of filtering and as a result, 74 primary studies were selected and investigated. However, the current data privacy attacks and threats in MCC were identified, and the current privacy solutions were proposed to preserve personal data protection in the MCC.

In the conducted systematic mapping study, the existing data privacy attacks and threats in mobile cloud computing were identified. The outcome indicated that the most common attacks and threats presented are unauthorized attacks and threats, which is illustrated in 18% of the chosen primary studies. Followed by data privacy, the leakage of the user privacy, misuse of the data, and an untrusted cloud service provider with 15%, 13%, and 11% of the selected primary studies, respectively. Moreover, disclosing the information or the data, the man-in-the-middle attacks with 6% and 5% of the selected primary studies. Furthermore, the result of SMS shows that there is a lack of studies on internal attacks, eavesdropping attacks, internal multi-layer attacks, data breach threats, inference attacks on user privacy, and improper security practices and policies in some locations.

In the conducted SMS, the existing data privacy solutions projected to preserve personal data protection in mobile cloud computing were identified. The result identified that the studies concentrated on encryption, authentication, and access control solutions

in 50%, 28%, and 19% respectively on the selected primary studies. Moreover, this study noted that authors had proposed trust solutions in the MCC field and currently, only two primary studies demonstrated trust solutions. Furthermore, the results of the SMS have not shown any proposed solution that utilizes the PbD solution to preserve PPDP in the MCC.

Furthermore, this Chapter presented related work in information systems security and privacy and research gaps of PPDP in the MCC. The next chapter presents the theoretical background of this study.

CHAPTER 3: THEORETICAL PERSPECTIVE

This chapter introduces the theoretical perspective of this study, including the theoretical perspective of PPDP in the MCC and theories associated to information systems security and privacy. This chapter also presents a comparative analysis on theories or models and determinants of preserving PPDP. Furthermore, this chapter shows the conceptual framework and hypothesis.

3.1 Theoretical Perspective of Privacy and Personal Data Protection in Mobile Cloud Computing

Referring to the analysis of the privacy and personal data protection (PPDP) in the literature on mobile cloud computing, the theoretical perspective is shown as follows; Theories used in research for information systems security and privacy, including the Technology Acceptance Model (Davis, 1989), Theory of Planned Behavior (TPB), Health Belief Model (HBM), and Theory of Reasoned Action (TRA). Moreover, a comparative analysis of theories including the Technology Acceptance Model (Davis, 1989), Theory of Planned Behavior (TPB), Health Belief Model (HBM), and Theory of Reasoned Action (TRA) was carried out. Also, Determinants are used in the literature to investigate information systems' security and privacy. Those determinants that influence the preservation of PPDP in the MCC were demonstrated in this research. Finally, a proposed conceptual framework and hypotheses were formulated.

In the following sections, the theoretical perspective of this study is presented.

3.2 Theories used in Research for Information Systems Security and Privacy

Before presenting the theories applied in this research for information systems security and privacy, it is essential to clarify the variance between privacy and security. Research reported that security is about protecting data, whereas privacy is about protecting users' identities. On the other hand, the specific differences are more complicated, and there can

surely be an area of overlap between the two. Hence, privacy and security go hand in hand to protect the data.

This section highlights some of the theories that have been broadly utilized when exploring or designing how individuals respond to technological change in information systems security and privacy. Furthermore, the theories selected from the literature review emphasized information system security and privacy behavior. The reason why those theories were chosen is to address the likelihood of behavior change in the conceptual framework. The selected theories include the Technology Acceptance Model (TAM); which is the most extensively applied theory to describe the consumer acceptability of information technology (Vatka, 2019; Kim & Park, 2012), Theory of Planned Behavior (TPB); one of the popular predictive persuasion theories out there (Kim & Park, 2012), Theory of Reasoned Action (TRA); that is best-known theoretical behaviors and intentions (Hartanti et al., 2021), and Health Belief Model (HBM); which is well-known as social cognition models for describing health behavior change (Kim & Park, 2012).

3.2.1 Technology Acceptance Model

Technology Acceptance Model (TAM) is known as a theoretical framework utilized to help to comprehend the user's intention of rejection or acceptance of the technology (Davis, 1989), that is, what causes potential recipients to reject or agree on the use of information technology. Also, the technology acceptance model is an adaption of the Theory of Reasoned Action (TRA) to the domain of Information Security (IS), developed by Davis in 1985 (Davis, 1989), where the main tool at that time for businesses was computers almost all over the world. Technology acceptance is known as 'the psychological state of an individual in the voluntary or intentional use of a particular technology." (Akinde, 2016). Davis began developing the model with two main issues as follows. First, Davis has proposed a model to understand the user acceptance process by

offering fresh theoretical insights into designing and implementing an IS successful. Secondly, David provided a theoretical basis for practical user acceptance testing to provide useful information considering the users' perspective for systems designers (Davis, 1989), to design new systems to guesstimate an effective new system before its implementation. TAM offers a basis for tracking how external variables affect perceptions, attitudes, intentions of utilizing a specific technology, and the actual use of the technology (Akinde, 2016).

TAM assumes that the utilization of information systems is defined by behavioral intentions. Conversely, behavioral intentions depend on people's attitudes towards using the system and their perceptions of its usefulness. According to Davis, personal attitude is not only the factor that defines their utilization of the system. It is also based on its possible influence on their performance (Tavallaee et al., 2017). Therefore, even if employees do not welcome information systems, they are more likely to use them if they recognize that they will improve their performance in the workplace. TAM also assumes a direct association between perceived ease of use and perceived usefulness. Both systems provide the same functionality and users will discover that an easy-to-use system is more helpful and convenient (Tavallaee et al., 2017).

As seen in Figure 3.1, behavioral intention to utilize directly impacts actual system use. The behavioral intention to use is represented as a purpose of ease of use and perceived usefulness (Davis et al., 1989). Also, as presented in Figure 3.1, the attitude consists of two constructs; the first is perceived usefulness, known as the user's belief that employing a certain technology would improve their professional performance (Davis, 1989). On the other hand, the second construct is the perceived ease of use, which states that users believe that employing a particular technology would decrease their time and effort (Davis, 1989).

Although the TAM model has some major weaknesses in proper capturing and explanation of an individual's behavioral intention, it is one of the most often applied theories for interpreting user behavior and technology adoption (Vatka, 2019); even though the perceived ease of use and usefulness are variables that aid in observing and using different IT, the beliefs do not completely interpret users' relationship to a newly emerging IT, such as Internet banking (Vatka, 2019).

TAM represents a significant theoretical contribution to the comprehension of technology acceptance and user behavior (Akinde, 2016; Malhotra & Galletta, 1999). Also, it was utilized as the theoretical foundation for several experimental research on user acceptance and technology use behavior (Tubay, 2021; Shana & Abulibdeh, 2017; Eltayeb & Dawson, 2016; Opitz et al., 2012; Davis, 1989). Due to its robustness and simplicity in interpreting user acceptance of technology, the technology acceptance model has gained widespread experiential support since its establishment (Liu & Ma, 2006) and has gained extensive acceptance as a framework for interpreting technology acceptance decisions by the users (Akinde, 2016; Hong et al., 2002).

TAM is popular as a theoretical framework since it is a theory designed to implement and accept Information and Communication Technology (ICT). The IS research community owns this theory, and theories in this field are rare (Otieno et al., 2016). TAM provides a clear and proven framework for ICT adoption and implementation research (Otieno et al., 2016). Another advantage of TAM is its simplicity, which is achieved by excluding social and organizational factors from the theoretical scope (Otieno et al., 2016). Conversely, focusing on the weaknesses, TAM has omitted social and organizational factors in its construction, which are very important in influencing technological innovation and the adoption of ICT (Otieno et al., 2016). In addition, many extensions of TAM have failed to deepen the theory in explaining the basic concepts more deeply, for example, accurately explaining the meaning of ease of use or perceived

usefulness (Otieno et al., 2016). Moreover, research reported that TAM fails to capture the variety of constraints and user mission environments. Also, in TAM, several essential theoretical constructs are ignored (Olushola & Abiola, 2017).

Most TAM research reaffirms the importance of perceived usefulness without spending much effort studying what makes the system useful (Jokonya, 2017). Moreover, TAM's dominance as a paradigm has been criticized by some researchers for creating a narrow slice of the IT adoption area. The perceived usefulness of the TAM structure is also subjective because individuals have different views on the utility of technology (Jokonya, 2017). TAM is overemphasized as a dependent variable, which prevents researchers from investigating other important user behaviors. The disadvantage of TAM is that the organizations of IT are constantly changing, making it less relevant (Jokonya, 2017).

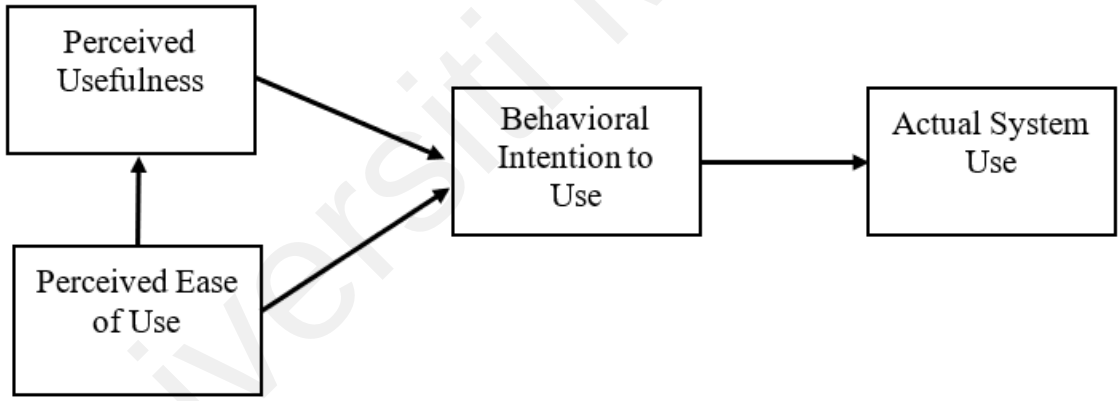


Figure 3.1: Theoretical Framework of TAM

3.2.2 Theory of Reasoned Action

The theory of reasoned action (TRA) was formed by Ajzen and Fishbein (1975) to comprehend human attitudes and intentions towards a particular behavior. Based on the Theory of Reasoned Action, an individual's behavior is determined through behavioral intentions, which result from a person's attitude regarding behavior and subjective norms surrounding performing the actions. Also, attitude towards behavior is referred to negative or positive emotions of the individual about conducting a behavior. This is

calculated by evaluating a person's beliefs about the repercussions of one's activities and a desire for such consequences (Arpaci, 2019). It is used primarily to investigate how attitudes consciously affect personal behavior and to investigate attitude formation from cognitive information. The main supposition of the model is that people are rational and take into account the importance and consequences of the action by aggregating the information obtained before taking action (Lee et al., 2016). TRA can be extended to conceptualize human behavior patterns in decision-making strategies related to innovations or the use of new technologies. It can explain whether individual behaviors are defined by behavioral intentions. In addition, behavioral intentions are defined as a person's attitude toward subjective standards surrounding behavioral performance, their sense of ease of action, and behavior (Otieno et al., 2016).

As shown in Figure 3.2, behavioral intention directly affects actual behavior use, and it is shaped as an outcome of attitude and subjective norms. According to the theory of reasoned action, attitudes are a belief function. Any person who has a belief that engaging in a particular behavior will result in good results, in most cases, will be positive towards this behavior (Lada et al., 2009). Conversely, a person who has a negative opinion about this behavior will often have a negative attitude (Lada et al., 2009). The belief underlying a person’s behavioral attitude is called behavioral belief (i.e., the act of showing your data or hiding it from others). The subjective norm is also a feature of the belief that a particular person or group of people should consider whether they should perform the behavior or not. That belief that forms the subjective norm of a person is mentioned as normative belief (Lada et al., 2009). Sheppard et al. (1988) argued that in the chosen scenario, the option is made by the strongest attitude towards the behavior and the subjective norm (Prachaseree et al., 2021). So, if the product features or attributes of items in the choice set are quite comparable. Likely, attitudes toward behavior and subjective standards are not different. However, the accuracy of choice prediction may not be valid, so the

researchers agree and recommend that "TRA should be amended or extended" (Prachaseree et al., 2021; Albarq & Alsughayir, 2013). The TPB theory is a well-known example of TRA extension. Due to the limitations of TRA in explaining behavior concerning voluntary control, Ajzen (1985) proposed a new theory by adding perceived behavioral control, which is a person's belief in controlling behavior's performance (Prachaseree et al., 2021; Madden et al., 1992). Thus, it can be said that "the idea of planned behavior is an extension of the theory of reasoned action" (Prachaseree et al., 2021).

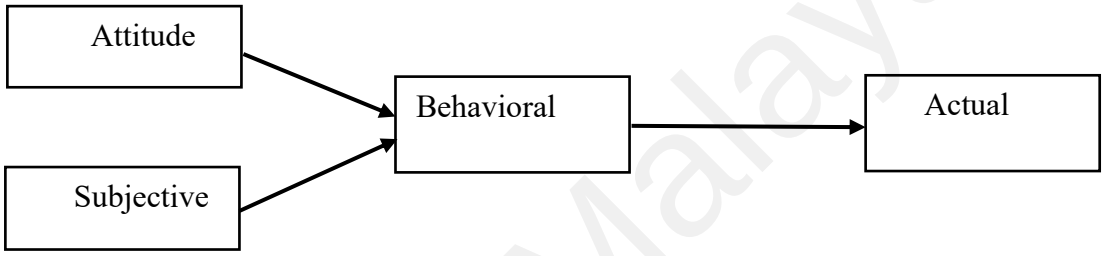


Figure 3.2: Theoretical Framework of TRA

3.2.3 Theory of Planned Behavior

Various theories, for instance, the theory of planned behavior (TPB) and the theory of reasoned action (TRA), were borrowed from different disciplines and applied to information systems. The information systems discipline pays particular attention to the development strategies of the information systems, and their usage of a mechanism in the real world (Jokonya, 2017; Al-Lozi & Papazafeiropoulou, 2012). Understanding complex problems in information systems lead to the borrowing of theories from established disciplines to help in the understanding of the technology and process interactions between individuals and organizations. One of the most popular theories for grasping human performance in information systems is the theory of planned behavior (Jokonya, 2017).

Based on the preceding work done by Ajzen and Fishbein, Ajzen expanded the theory of reasoned action. In the TPB theory, Ajzen provided another factor to affect the intent

of the behavior, namely the Perceived Behavior Control (PBC), to enhance the previous model. TPB is developed from the principle of aggregation. The model assumes that a collection of specific behaviors is sometimes more effective in predicting attitudes and other characteristics than analyzing perception control alone (Raygor, 2016). In summary, TPB endeavors to address individual motivational factors in a single context to explain the overall performance of specific behaviors (Raygor, 2016; Ajzen, 1991). According to Ajzen, Perceived Behavioral control is referred to as reflecting the belief about having arrived at the opportunities and resources necessary to execute a particular behavior. As illustrated in Figure 3.3, PBC will impact Behavioral Intention and Behavior (Taylor & Todd, 1995). The intention of the person to achieve a particular behavior is still at the center of the theory (Ajzen, 1991).

The author aimed to develop the Theory of Reasoned Action (TRA) model, taking into account restrictions like norms versus attitudes, and when the intent to act is implemented, an individual may act without any limitation (Ajzen, 1991). The author stated that intention point to how hard people are preparing to attempt and how much exertion they will make to carry out their behavior (Ajzen, 1991). As a universal rule, "the stronger the intention to engage in a behavior, the more likely should be its performance" (Ajzen, 1991). For example, suppose a person shows a strong intention to practice, such as practicing information security technology and having the in-demand capacity and means. In that case, they are more expected to do the behavior. In other terms, the TPB theory emphasizes the effect of behavioral control and intention on behavior, and it states that the behavior of users can be foretold through their intention. (Ajzen, 1991, 1988).

Figure 3.3 shows that there are three main factors, which are attitude toward the behavior as previously defined in the TRA model, which indicates the stage to which a person has a negative or positive assessment of the behavior in question. As previously described in the TRA model, the second factor is subjective norms. It can be described as

the perceived social influence to either achieve the behavior or not. Finally, the perceived behavioral control indicates the perceived difficulty or ease in executing the behavior, which is supposed to reflect the previous knowledge, potential impediments, and hurdles (Ajzen, 1991, 1988). TPB addresses the weaknesses of its predecessor TRA by allowing predictive behavior to be incompletely controlled by will. To address the weaknesses of its predecessor, TPB uses Perceived Behavior Control (PBC) as an extra determinant of human motivation and intentions for TRA. The addition of PBC is based on the fact that people may not be able to control their expected behavior fully, especially in an unstable and uncontrolled external environment (Jokonya, 2017). Therefore, adding perceptual behavior control enables TPB to predict and check human intentions and behaviors in situations where individuals may be unable to handle their behavior (Jokonya, 2017). Moreover, the three main factors are considered as the factors affecting behavioral intention (Ajzen, 1991, 1988). The more favorable attitudes and subjective norms can be expressed as the stronger perceived control, the more powerful the person's intention to engage in the behavior in question (Jokonya, 2017). The bottom line is that if people have sufficient actual control over their behavior, they realize their intentions when an opportunity arises. Some researchers believe that human behavior is guided by different subjective probabilities, including belief in behavioral consequences, belief in normative expectations of others, and belief in the existence of constructs that can promote or hinder behavioral performance (Jokonya, 2017; Ajzen, 1991).

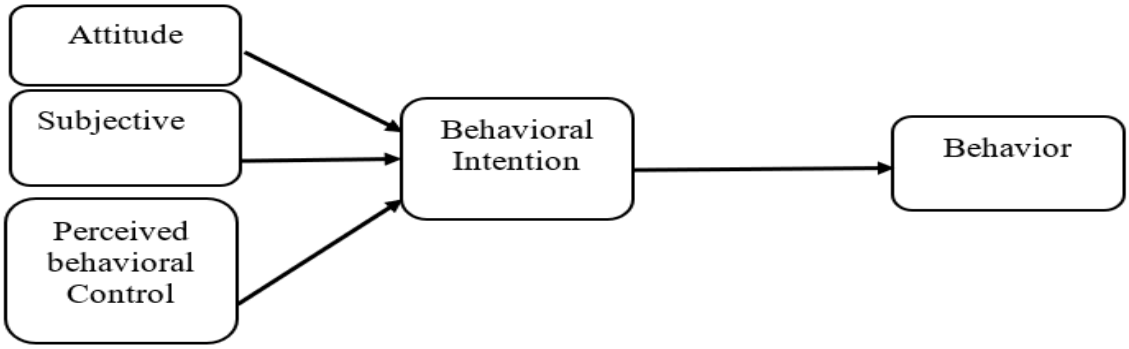


Figure 3.3: Theoretical Framework of TPB

3.2.4 Health Belief Model

This section illustrates the literature review of the Health Belief Model that consists of the history of the HBM, HBM Assumptions, and HBM components, as well as an individual's perceptions and HBM concepts.

3.2.4.1 History of HBM

In the early 1950s, a Health Belief Model (HBM) was established by psychologists, Irwin Rosenstock, Stephen Regels, and Godfrey Hochbaum employed in the US Public Health Service in the United States (Tarkang & Zotor, 2015; Cummings et al., 1978). The Public Health Services do not have a high value nowadays, such as the patient's symptoms, aftercare, or doctor-patient contact (Rosenstock, 1974). The HBM uses theories of expected value to explain healthy behaviors from a social psychology perspective (Mikhail & Petro- Nustas, 2001; Kronenfeld & Glik, 1991). HBM is a conceptual framework of health behaviors developed to guide and understand people's failure in adopting the screening tests or disease prevention strategies for early disease detection, which is most widely used to understand health behavior (Claar & Johnson, 2010). The focus of the theory is on the behaviors of people who (1) did not suffer the signs or consequences of a certain illness and (2) are aware of the proposed preventive measures (Williams et al., 2014). Subsequent use of the health belief model is for patients' responses to symptoms and compliance with medical treatments. The HBM proposes that the belief of an individual in the personal threat of a disease or illness combined with the belief of a person in the usefulness of the prescribed health behavior or action will determine the likelihood that an individual will accept the behavior (Jones et al., 2015).

3.2.4.2 HBM assumptions

The HBM developers set out the following assumptions related to the implementation of health-related activities (Tarkang & Zotor, 2015):

a) The HBM assumes that individuals will take action associated with their health if they feel that a harmful health problem can be averted. However, it is important to assist people to understand that they can avoid disease, and that will only happen if they have a true understanding of the problem. Thus, it is only after one knows this that one would undertake preventive action.

b) The HBM also assumes that an individual will undertake preventive action when an individual has a positive belief that a harmful health problem can be prevented by carrying out the suggested action. The individual is required to know the benefits that one will gain through active behavior. If an individual sees no benefit, it would be hard for one to take or sustain the required action.

c) The HBM assumes that a person is having health-related activities if they think that the recommended action can be taken effectively. It needs a person to feel assured that he or she can carry out the advised action, which necessitates that the individual has the requisite expertise and abilities to carry out the required action (s) in a supportive environment.

3.2.4.3 HBM components

The HBM has three primary components (Tarkang & Zotor, 2015):

a) The individual's perceptions about health.

b) The adjusting factors contain structural variables, demographic, and socio-psychological.

c) The advantages of adopting preventive actions.

(a) ***The individual's perception***

Individual perception is an individual's thought about one's vulnerability to illness, and positivity to the severity with which he or she considers the perceived threat of disease (Onega, 2000). A person's perception changes because of the newly gained knowledge,

which in great measure results in a minimization of the disease threat (Tarkang & Zotor, 2015).

*(b) **Modifying factors***

Modifying factors such as structural variables, socio-psychological, and demographic can impact an individual's perceptions and thus indirectly affect behaviors. For example, socio-demographic factors, such as educational status, could influence the individual's perceptions of susceptibility to and seriousness of suffering ill impacts (Vatka, 2019).

*(c) **Variables influencing the likelihood of initiation and preservation of action***

The likelihood of action refers to perceived barriers minus the perceived benefits of taking action, which is equivalent to the likelihood of acting that alter the behavior (Vatka, 2019; Tarkang & Zotor, 2015). For this research, these factors point to a mobile cloud computing user-perceived benefit in utilizing MCC that used privacy by design minus the perceived barriers of using MCC without privacy by design.

3.2.4.4 Concepts of HBM

The HBM is a theory of value expectation with 2 values: The first value is the desire to prevent or recover from the disease, and the second value is the belief that health actions accessible to a person will avoid unwanted consequences (Onega, 2000).

According to Rosenstock (1974), the trait of the HBM was that if one were to desire to combat disease, he would have to be believed (Tarkang & Zotor, 2015):

a) He or she was susceptible to it.
b) If he had been infected with the illness, there would have been consequences in his life, at least to some degree.
c) Taking some clear counter-measures would be helpful, as it would minimize susceptibility to lessen or condition the effects to avoid barriers like pain, embarrassment, convenience, or cost.

As shown in Figure 3.4, the predictive value of health belief model constructs includes perceived benefits, cues to action, perceived barriers, and perceived threat, which combine the perceived susceptibility and the perceived severity (Edwards, 2015; Orji et al., 2012; Ng et al., 2009; Rosenstock, 1974).

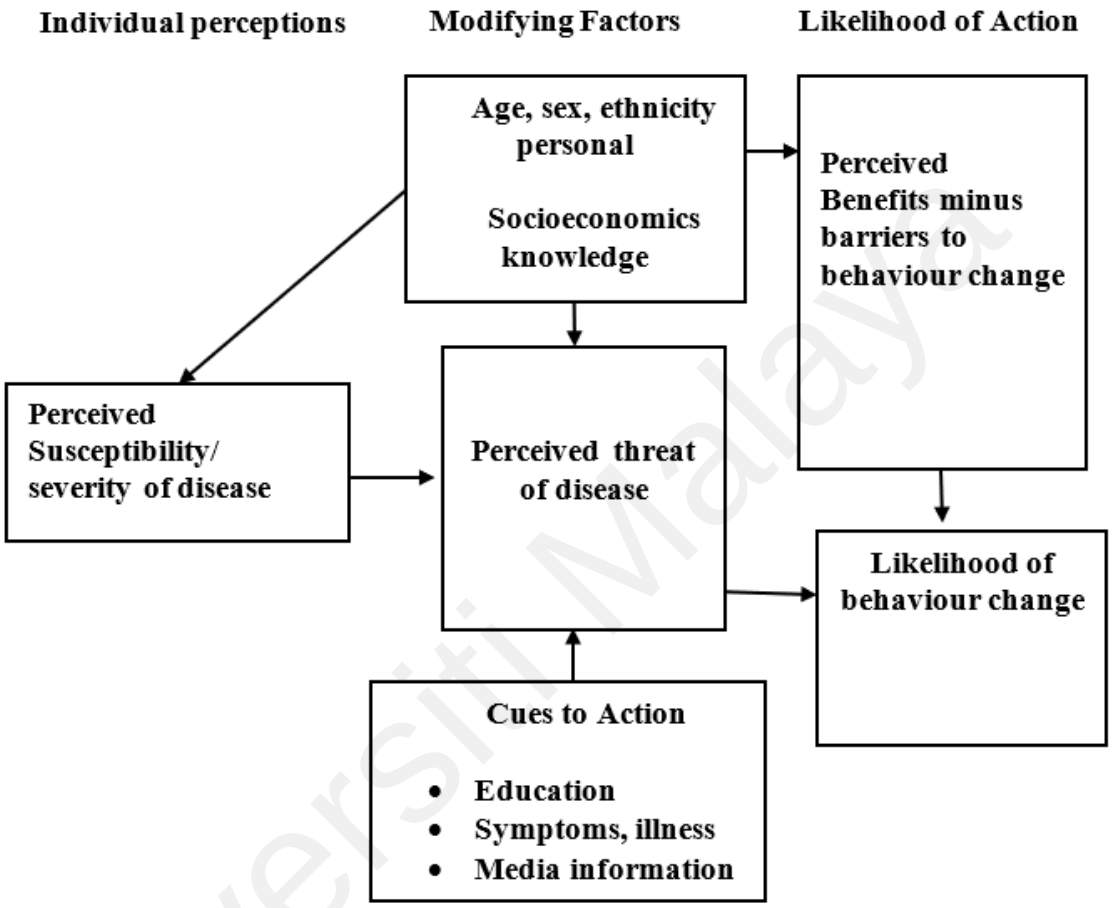


Figure 3.4: Health Belief Model (Rosenstock, 1974)

(a) ***Perceived benefits***

Perceived benefits (P.BEN) are defined as the person's thoughts on the validity of the advised action to reduce the threat or severity of the effect (Tarkang & Zotor, 2015). The individual is required to believe that by performing a specific action. This action will assist the person in preventing or at least avoiding a problem from happening. This belief gives the person the feeling of taking action because of the projected results (Tarkang & Zotor, 2015).

(b) ***Perceived Barriers***

Perceived barriers (P.BAR) refer to the negative sides of specific health actions. These might act as limitations considering a person behaving according to the recommended behavior. For instance, if the cost of the treatment is expensive, it may have annoying symptoms or be inconvenient (Glanz et al., 2008; Rosenstock, 1974). It is only when people understand that they can work with barriers like duration, costs, the complexity of the wanted behaviors, and access to facilities that would help in the implementation and retention of the needed actions that they would be able to take the important actions (Polit & Beck, 2004).

(c) ***Cues to Action***

Cues to action refer to occurrences or interactions that motivate a person towards action (Tarkang & Zotor, 2015; Groenewold et al., 2006). Cues to action occur when an individual is compelled to take appropriate action after realizing that such an individual has the power to do so. The recommended action would help one to cope with the anticipated barriers. Thus, it requires a person's spur to be willing in complying with the treatment or recommended action to have a concern about health problems (Polit & Beck, 2004). Also, one should be ready to seek health care and accept it to participate in helpful health actions (Polit & Beck, 2004). It has been confirmed by a couple of studies that if an individual has been affected before, they might detect upcoming concerns more easily (Vatka, 2019; Dodel & Mesch, 2017).

(d) ***Perceived Threat***

As presented in the literature, the perceived threat affects the person's intent to perform health-related behavior (Edwards, 2015). According to Glanz et al. (2008) and Edwards (2015), the perceived threat is presented by the incorporation of perceived susceptibility and perceived severity to the condition or disease.

a) Perceived Severity (Seriousness): This is associated with an individual's perception of the severity of health problems (Vatka, 2019). When one realizes one's vulnerability to a specific issue or disease, it is unnecessary to encourage oneself to adopt the recommended preventive measures because the condition will have serious health and social consequences (Tarkang & Zotor, 2015). It is when one recognizes the extent of a condition of negative consequences that one can take the actions obligatory to avoid or prevent those bad consequences (Tarkang & Zotor, 2015).

b) Perceived Susceptibility (Vulnerability): Perceived susceptibility is referred to as an individual's perceptions about the likelihood of having a health problem (Tarkang & Zotor, 2015; Groenewold et al., 2006). An individual's perception that a health condition is directly important may lead to taking the necessary action to avoid or prevent health problems. To do so, there need for behaviors that enhance the person's perception of one's susceptibility to the health problem (Tarkang & Zotor, 2015). For example, a woman should know that she has a possible risk of having breast cancer before she is prepared to undergo obtained mammography (Glanz et al., 2008; Rosenstock, 1974).

3.3 Comparative Analysis of Theories or Models

A comparative analysis of theories or models is used to identify the available theories to be utilized in this research. Table 3.1 shows a comparative analysis of the theories or models. The table shows four theories and highlights their components or features, description, strength, and limitations, as well as the need for the theory or model for this research. Interestingly, those theories are used in research for information systems security and privacy.

Table 3.1: Comparative analysis of theories or models

Model Name	Component/ Features	Description	Strength	Limitation	The Need for the theories for this research
Technology Acceptance Model (**TAM**) Authors: (Davis, 1989)	• System usage • Behavioral intention to use • Perceived ease of use • Perceived usefulness	A theoretical framework is utilized to help understand the user's intention to reject or accept the technology (Davis, 1989).	Focused on behavioral elements	• It contains some major limitations in fully explaining and capturing an individual's behavioral intention. • The beliefs do not demonstrate the relationship of users to newly emerging IT (Wang et al., 2003).	This model is not needed because the beliefs do not interpret the relationship of users to newly emerging IT. (Wang et al., 2003).
Theory of Reasoned Action (**TRA**) Authors: (Fishbein & Ajzen, 1975)	• Attitude toward • Behavior • Behavioral intention • behavior • Subjective norm	To comprehend human attitude and intentions towards a particular behavior.	Focuses on behaviors that people decisively enact	This model constraint are time, unconscious habits, organizational or environmental limits, and limited ability will limit the freedom to act.	This model is not utilized in the study because the model has constraints likeability, limitations, organizational, environmental limits, or time.
Theory of Planned Behavior (**TPB**) Authors: Ajzen (1985)	• Behavior • Behavioral intention • Attitude toward behavior • Perceived behavioral control • Subjective norm	To predict an individual's desire to participate in an activity at a specific time and place.	Explain and predict a wide assortment of behaviors and intentions.	An incapability to consider economic and environmental influences. The theory does not address what is known as the action phase, which is concerned with the translation of intention into conduct.	This model is not used in the study because it does not address what is known as the action phase, which is concerned with the translation of intention into behavior.
Health Belief Model (**HBM**) Authors: (A team from the U.S. Public Health Service (the 1950s))	• Perceived threat • Perceived susceptibility • Perceived severity • Perceived barriers • Perceived benefits • Cue to action	• Defines health behavior as an indication of a person's health values. • The model presupposes that an individual's health-seeking behavior is driven by the individual's	Focus on the behaviors of people	• It is predicated on the premise that everyone has access to the same amount of knowledge about the sickness or condition. • It assumes that cues to action are	• The study utilized HBM because the model has factors such as the perceived threat that could measure the causes and impacts. • In addition, measuring cues to action

		knowledge of the risk provided health issues and the perceived utility of actions intended at reducing the threat		widespread to encourage individuals to take action and that the primary goal of the decision-making process is "health" activities.	distinguishes the health belief model from TAM, TPB, and TRA.

3.3.1 Determinants of Preserving Privacy and Personal Data Protection

In this investigation, the conducted Systematic literature review (SLR) has identified determinants that are used for preserving privacy and security in information systems. The SLR methodology is presented in Sub-section 4.2.2.

Table 3.2 shows the selected primary studies in the SLR and the identified determinants with related theories in the selected primary studies. As illustrated in Table 3.2, a total of 37 determinants in 19 studies were identified. The identified determinants are associated with their related theories to determine the most used determinants in the investigations related to this work. The results show that most used determinants are demonstrated using the health belief model (HBM).

Table 3.2: Selected primary studies in the SLR and the identified determinants with related theories

#	Author	Determinants	Research domain	Related theories
1	(Ng et al., 2009)	Perceived susceptibility.	Computer security behavior.	HBM
		Perceived barriers.		HBM
		Perceived benefits.		HBM
		Perceived severity.		HBM
		General security orientation.		Contributed by the authors
		Self-efficacy.		HBM
		Cues to action.		HBM
2	(Claar et al., 2010)	Cues to action.	Computer security usage.	HBM
		Perceived barriers.		HBM
		Perceived benefits.		HBM
		Perceived severity.		HBM
		Self-efficacy.		HBM
		Perceived vulnerability.		HBM
3		Perceived benefits.		HBM

#	Author	Determinants	Research domain	Related theories
	(Humaidi & Balakrishnan, 2012)	Co-workers interaction.	Information security.	Contributed by the authors
		Cues to action.		HBM
		Self-efficacy.		HBM
		Perceived risk.		Contributed by the authors
		Perceived Integrity.		Contributed by the authors
		Perceived susceptibility.		HBM
		Perceived severity.		HBM
		Perceived barriers.		HBM
		Conscientiousness.		Contributed by the authors
		Cultural assumptions and beliefs.		Contributed by the authors
		Perceived security.		HBM
		Perceived security countermeasure.		Contributed by the authors
		Perceived internal threat.		Contributed by the authors
		Perceived ease of use.		Contributed by the authors
		Perceived trust.		Contributed by the authors
4	(Williams et al., 2014)	Susceptibility.	Security behaviors.	HBM
		Severity.		HBM
		Benefits.		HBM
		Barriers.		HBM
		Cue to action.		HBM
		Self-efficacy.		HBM
5	(Humaidi & Balakrishnan, 2014)	Perceived benefit.	User's compliance behavior towards health information system's security policies.	HBM
		Perceived severity.		HBM
		Perceived susceptibility.		HBM
		Perceived barriers.		HBM
		Self-efficacy.		HBM
		Cues to action.		HBM
		Perceived working experience.		Contributed by the authors
6	(Sekyere, 2015)	Perceived Severity.	Security behavior.	HBM
		Self-efficacy.		HBM
		Perceived benefit.		HBM
		Perceived Susceptibility.		HBM
		Cues to action.		HBM
		Perceived barriers.		HBM
7	(Hassan & Ismail, 2015)	Experience.	Information security.	Contributed by the authors
		Organizational IS Policy.		Contributed by the authors
		Perceived Threat.		HBM

#	Author	Determinants	Research domain	Related theories
		Cultural Assumption and Belief.		Contributed by the authors
		Perceived Susceptibility.		HBM
		Trust.		Contributed by the authors
		Perceived Benefits.		HBM
		Perceived Severity.		HBM
		Self-efficacy.		HBM
8	(Humaidi & Balakrishnan, 2015)	Perceived benefit.	Security policies compliance behavior.	HBM
		Perceived susceptibility.		HBM
		Self-efficacy.		HBM
		Perceived severity.		HBM
		Management support.		Contributed by the authors
		Information security awareness.		Contributed by the authors
		Perceived trust.		Contributed by the authors
9	(Ameme & Yeboah-Boateng, 2016)	Security awareness.	User behavior.	Contributed by the authors
		Severity to the security threat.		Contributed by the authors
		Exposure to security threats.		Added by the authors
		Perceived benefits.		HBM
		Self-Efficacy.		HBM
10	(Hsu, 2016)	Disposition to value the privacy.	Intention to upload personal health data.	Contributed by the authors
		Perceived benefits.		HBM
		Self-efficacy.		HBM
		Perceived severity.		HBM
		Specific information privacy concerns.		Contributed by the authors
		Perceived vulnerability.		HBM
		Perceived barriers.		HBM
11	(Shin et al., 2016)	Perceived benefits.	Privacy behavior.	HBM
		Perceived severity.		HBM
		Perceived probability.		Contributed by the authors
		Perceived barriers.		HBM
		Self-efficacy.		HBM
		Privacy protection.		Contributed by the authors
12	(Dodel & Mesch, 2017)	Perceived benefits.	Anti-virus preventive behavior.	HBM
		Perceived susceptibility.		HBM
		Perceived barriers.		HBM
		Perceived severity.		HBM
		Beliefs about self-efficacy.		Contributed by the authors

#	Author	Determinants	Research domain	Related theories
		Previous malware cyber-victimization experience.		Contributed by the authors
		Cues to action		HBM
13	(Schymik & Du, 2017)	Perceived vulnerability.	Email security behavior.	HBM
		Perceived barriers.		HBM
		Self-efficacy.		HBM
		Perceived benefits.		HBM
		Perceived severity.		HBM
		Prior experience.		Contributed by the authors
		Cues to action.		HBM
14	(Anwar et al., 2017)	Perceived vulnerability.	Cyber security behavior.	HBM
		Perceived barriers.		HBM
		Perceived benefits.		HBM
		Perceived severity.		HBM
		Response efficacy.		Contributed by the authors
		Self-efficacy.		HBM
		Cues to action.		HBM
		Peer behavior.		Contributed by the authors
15	(Bikoro et al., 2018)	Perceived vulnerability.	Cyber security use and behavioral intention.	HBM
		Perceived barriers.		HBM
		Cues to action.		HBM
16	(Koloseni & Gan, 2019)	Perceived benefits.	Information security behaviors.	HBM
		Perceived severity.		HBM
		Perceived barriers.		HBM
		Perceived susceptibility.		HBM
		Cues to action.		HBM
		Self–efficacy.		HBM
		Information security habit.		Contributed by the authors
17	(Schymik et al., 2019)	Perceived severity.	LBS security behavior.	HBM
		Cues to action.		HBM
		Perceived barriers.		HBM
		Perceived vulnerability.		HBM
		Perceived benefits.		HBM
		Self-efficacy.		HBM
		Prior experience.		Contributed by the authors
18	(Al-diabat, 2019)	Perceived susceptibility	Information computer security.	HBM
		Perceived barriers.		HBM
		Cues to action.		HBM
		Perceived benefits.		HBM
		General security orientation.		Contributed by the authors
		Perceived severity.		HBM

#	Author	Determinants	Research domain	Related theories
		Self-efficacy.		HBM
19	(Vatka, 2019)	Perceived susceptibility.	Data privacy behavior.	HBM
		Perceived benefits.		HBM
		Self-efficacy.		HBM
		Perceived seriousness.		HBM
		Perceived barriers.		HBM
		Cues to action.		HBM

As shown in Table 3.2, for the determinants, the perceived benefits, perceived severity, cues to action, perceived susceptibility, and perceived barriers are presented in the original constructs in HBM (Rosenstock, 1974). On the other hand, a construct termed self-efficacy is presented as an individual's self-confidence in their skills or capability to execute a behavior. In addition, self-efficacy has been derived from social cognitive theory (Ng & Xu, 2007), which refers to a person's reactions to the difficulties inherent in changing persistent harmful behaviors (Chen, 2017; Ng & Xu, 2007). Self-efficacy was included in HBM in 1988 as an extra factor since a person's skill or ability to implement a specific action might affect an individual's likelihood to act (Koloseni, 2017). In this research, self-efficacy is not used because this study adapted the original contracts of health belief model according to Rosenstock (1974), as shown in Figure 3.4.

As shown in Table 3.3, the cues to action is the least used determinants in ISS, resulting in 14 studies. Followed by perceived barriers, perceived susceptibility, perceived severity, and perceived benefits resulted in 17 studies each.

Table 3.3: The most used determinants

Determinant	Number of studies
Cues to action	14
Perceived susceptibility	17
Perceived barriers	17
Perceived benefits	17
Perceived severity	17

3.3.2 Utilization of Health Belief Model as a baseline for proposing PbD framework

As shown in Table 3.3, there are similarities between HBM and the most used determinants in the domain. Accordingly, the following subsections present limitations of existing theories and models, highlight the utilization of the health belief model in information systems security and privacy and justify using HBM in the proposed PbD framework.

3.3.2.1 Limitations of existing theories and models

A comparative analysis of theories has been done, including the Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), and Health Belief Model (HBM). Although using those theories is interesting, however, researchers reported limitations inherent in those theories as follows:

a) Technology Acceptance Model: TAM is an appreciated theory (Tang et al., 2021); on the other hand, it is essential to report that research has noted that TAM has contained some major limitations in full explanation and capturing of an individual's behavioral intention. In addition, TAM has a belief that does not totally demonstrate the relationship of users to the newly emerging IT (Vatka, 2019). Therefore, TAM is not needed because the belief does not totally interpret the relationship of users to a newly emerging IT (Vatka, 2019).

b) Theory of Reasoned Action: Wonderfully, TRA is a wide range of utilized theories (Hartanti et al., 2021); however, some researchers argued that TRA has some constraints such as time, unconscious habits, organizational or environmental limits, and limited ability, which will limit the freedom to act (ODERO, 2021). So, TRA is not utilized in the study because the model has some constraints such as ability, limitations, organizational, environmental limits, or time.

c) Theory of Planned Behaviour: Magnificently, the research used TPB in multiple publications to solve many research problems; investigators believe that TPB is incapable of considering economic and environmental influences. Moreover, the theory does not address what is known as the action phase, which is concerned with the translation of intention into conduct (Momani & Jamous, 2017). In this research, TPB is not used because it does not address what is known as the action phase, which is concerned with the translation of intention into behavior.

d) Health Belief Model: Substantially, HBM is a widely applied theory (Kim & Park, 2012). However, it is assumed that everyone has access to the same information about the condition or illness. Moreover, it assumes that cues to action are widespread, encouraging individuals to take action and that the primary goal of the decision-making process is "health" activities.

3.3.2.2 Utilization of health belief model in information systems security and privacy

Several studies investigating security issues (Humaidi & Balakrishnan, 2015, 2012; Claar & Johnson, 2010; Ng et al., 2009) related to this research have been studied in the literature. In the study by Ng et al. (2009), HBM was used to study users' computer security behavior. Interestingly, the outcome of their study demonstrated that perceived susceptibility and perceived benefits are important determinants of email-related security behavior (Ng et al., 2009). In addition, another study presented a framework based on HBM to illuminate why people are not conscious of a hazard threat to warrant computer security software usage (Claar & Johnson, 2010).

Another study utilized surveys and interviews to measure the effect of security technology and awareness on the behavior of the users regarding health information on systems' security that is based on the Health Belief Model and PMT theory (Humaidi & Balakrishnan, 2012). The authors investigated the critical factors that affect users'

behavior toward information security in the health sector when the system allows them to share information between healthcare providers. The study concentrated on two factors; security technology and security awareness. They developed a conceptual framework based on PMT theory and HBM. The study expected that the result of the investigation would help recognize the new need for information system security and resolve existing problems in the information system security in organizations (Humaidi & Balakrishnan, 2012).

In addition, Humaidi and Balakrishnan (2015) studied the moderate influence of the health experience on the link among variables of the Health Information System Security Policies Compliance Behavior (HISSPC) model (Humaidi & Balakrishnan, 2015). The proposed model was verified by utilizing the PLS method, and the results pointed to the determination coefficient (i.e., R^2) (Humaidi & Balakrishnan, 2015).

Moreover, Williams et al. created the Security Belief model based on current health behavior models and is used to define information security behavior intentions (Williams et al., 2014). The model was empirically tested using a sample of 237 professionals (Williams et al., 2014). Also, the results show that the model is generally supported, especially in cue to action, severity, susceptibility, and benefits as the precursors to the desire to engage in preventative information security behavior (Williams et al., 2014).

Laing & Xue (2009) established the technology threat avoidance theory (TTAT). The study developed the TTAT to highlight the reason why users avert security threats. They researched to see how effective TTAT could understand the IT threat avoidance behavior of personal computer users on their model. In HBM, the model referred to perceived susceptibility and seriousness as direct determinants of perceived threat. The authors used protection costs to safeguard the effectiveness and perceived barriers as the same as perceived benefits in the HBM (Liang & Xue, 2010).

3.3.2.3 Justification for utilizing the Health Belief Model

As presented in the literature, HBM was used widely in information security domain studies (Koloseni et al., 2019; Humaidi & Balakrishnan, 2015; Williams et al., 2014; Humaidi & Balakrishnan, 2012; Claar & Johnson, 2010; Ng et al., 2009). This study adopts HBM for the following reasons:

a) Health belief models tackle personal human issues in order to model and evaluate the influences of illnesses (Harvey & Lawson, 2009; Champion & Skinner, 2008). Thus, the IS experts have used the health belief model in modeling and evaluating personal issues such as PPDP. Also, there are currently numerous PPDP determinants with causes and effects that can be fitted by the health belief model.

b) Health belief models can be utilized to measure the employment of privacy by design, considering visibility and location transparency to preserve PPDP in mobile cloud computing as the perceived threat and its underlying relationship to PPDP behavior for mobile cloud computing, which can be investigated by HBM.

c) The health belief model can enrich privacy by design in the MCC by providing cues to action (refers to experiences and applying location transparency for MCC storage location), where cues to action distinguish the health belief model from other theories such as TRA, TAM, and TPB.

d) The HBM can measure the perceived susceptibility and severity of PPDP threats in MCC. In addition, the HBM can also measure the benefits and barriers in executing PPDP behavior in MCC and cues to action to preserve PPDP in MCC.

3.4 Determinants that Influence the Preservation of Privacy and Personal Data Protection in Mobile Cloud Computing

In this research, a systematic method was applied to search the existing literature related to this research (Jaidka et al., 2013) as follows. Results of SLR (presented in Sub-section 4.2.2) revealed determinants that are used in the selected primary studies. The

determinants are aggregated in Table 3.2. In addition, a comparative analysis study was used to identify the theories to be utilized in this research. Table 3.1 shows the comparative analysis of theories or models. Furthermore, based on the most used determinants in the chosen primary studies in the SLR and the result of the comparative analysis, there are similarities between the most used determinants in the selected primary studies and HBM. As a result, the HBM was selected as the baseline for the proposed framework.

In this research, the health belief model is demonstrated in a conceptual framework that uses the predictive value of the original constructs of the health belief model (Rosenstock, 1974). Furthermore, cues to action in this particular framework are being modified to suit the contents of PbD to consider the visibility of location transparency. Also, the relation between the cues to the action of privacy by design considering visibility of location transparency directly with the PPDP behavior in the MCC is added.

Figure 3.5 illustrates the predictive value of the original constructs of the health belief model, containing the cues to the action of PbD, perceived barriers, perceived benefits, and the perceived threat that incorporates perceived susceptibility and perceived severity (Edwards, 2015; Orji et al., 2012; Ng et al., 2009; Rosenstock, 1974).

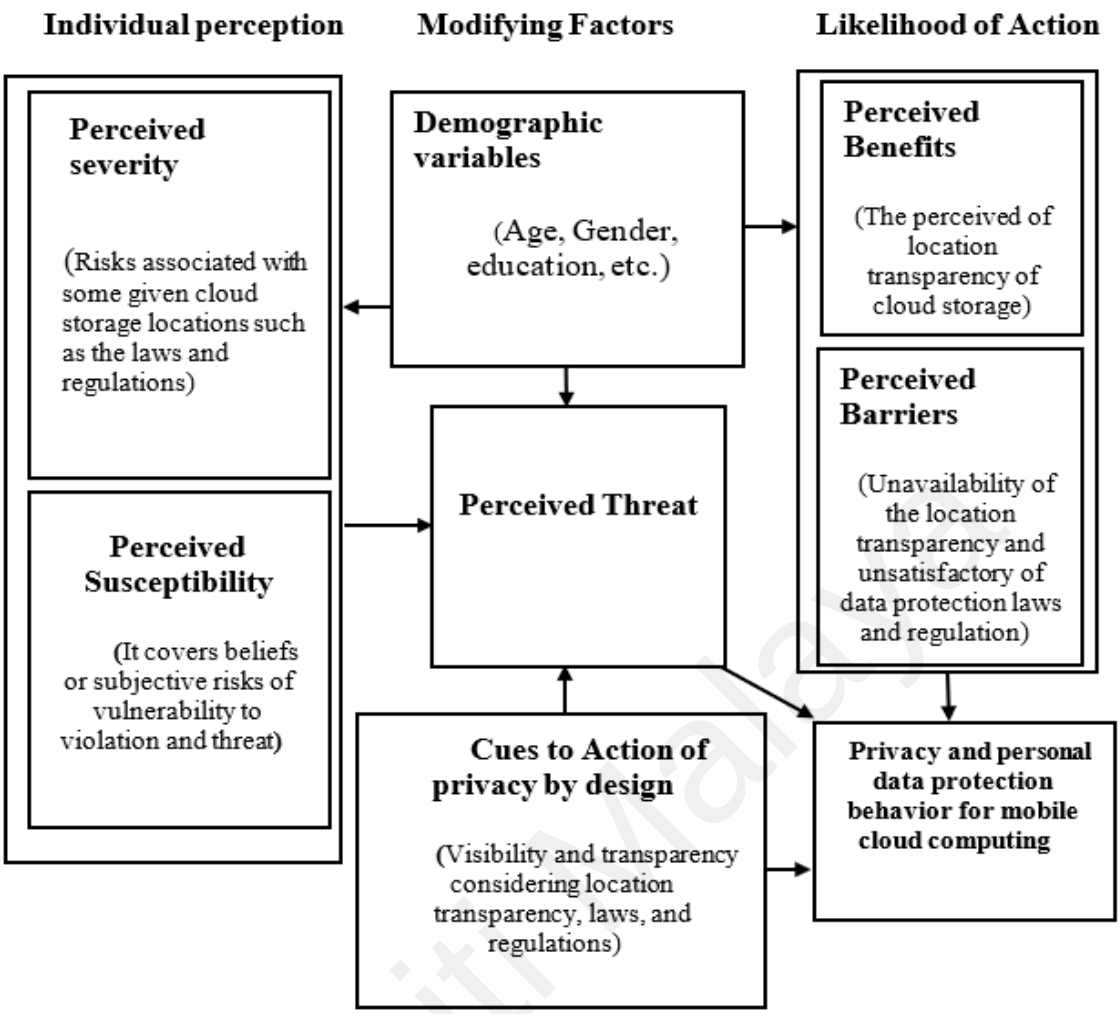


Figure 3.5: The proposed privacy by design framework

The following six constructs were used to design the privacy by design framework. Table 3.4 shows the determinants that were used in this research.

Table 3.4: Determinants used in this study

Construct	Definition	Relationship to the PbD in MCC
Perceived Benefits (P.BEN)	It refers to the alteration of an individual's behavior if there are some perceived benefits when adopting new behavior (Dodel & Mesch, 2017, Rosenstock, 1974).	In this context, it refers to the perceived benefits of location transparency of cloud storage.
Perceived Barriers (P.BAR)	It can be acted as a constraint when a person acts according to the recommended behavior. Although an individual may feel that a certain action is powerful in decreasing threats, the action may	MCC users ' perceived unavailability of location transparency and satisfactory in data protection laws and regulation.

	cause unnecessary pain or other inconvenience (Vatka, 2019).	
Cue to Action of privacy by design (CAPD)	Events that encourage people to change their behavior (Edwards, 2015). As confirmed by Dodel et al. and Vatka (Vatka, 2019; Dodel & Mesch, 2017), if an individual has been afflicted previously, they might discover upcoming concerns easier (Vatka, 2019; Dodel & Mesch, 2017).	Events that encourage people to alter their behavior when utilizing mobile cloud computing to store their personal data. If personal data has been afflicted when using mobile cloud computing due to the lack of location transparency, laws, and regulations, the person might not be encouraged to utilize the MCC to store his personal data.
Perceived Severity (P.SEV)	An individual's perception on how serious a health problem is (Vatka, 2019; Rosenstock, 1974).	Risks relate to some given cloud storage locations, such as the laws and regulations related to PPDP in mobile cloud computing.
Perceived Susceptibility (P.SUS)	An individual's perceptions about the likelihood of having a health problem (Tarkang & Zotor, 2015; Groenewold et al., 2006). An individual's perception that a health condition is directly important may lead to taking the necessary action to avoid or prevent health problems. To do so, there must be a behavior that enhances the individual's perception of one's susceptibility to the health problem (Tarkang & Zotor, 2015).	If a mobile cloud computing user sees the outstanding vulnerability to threat and violation, one is more likely to take further countermeasures according to their privacy and data protection behavior in mobile cloud computing.
Privacy and data protection behavior in MCC (PDPBMCC).	Considered the likelihood of changes in HBM.	The country's actions that hosted the actual cloud storage and their behaviors against malicious behavior and violation regarding mobile cloud computing.

3.4.1 Justification of why Incorporated Cues to Action with PbD

It is essential to mention that the HBM was selected as the baseline for the proposed framework. More importantly, the difference between the PbD framework and the HBM is highlighted below:

a) Cues to action in this particular framework are being modified to suit the contents of PbD to consider the visibility of location transparency.
b) The relation between the cues to action of privacy by design considering visibility of location transparency directly with the PPDP behavior in the MCC is added.

In this research, the following justification is presented to demonstrate why incorporating cues to action with PbD:

a) The cues to action as determinants present events that encourage people to change behavior (Yuen et al., 2020; Afandi et al., 2017; Dodel & Mesch, 2017; Edwards, 2015).
b) Applying privacy by design aims to assure all stakeholders operating according to the stated promises and objectives. Its parts and operations remain visible and transparent to providers alike and users (Pagallo, 2021; Semantha et al., 2020; Kolkowska & Kristofferson, 2016; Kolkowska, 2015).
c) As a motivation, visibility and transparency in PbD promote the utilization of a system that applies PbD (Bu et al., 2020; Yanisky-Ravid & Hallisey, 2019; Jusob et al., 2017; Everson, 2016). In other words, visibility and transparency in PbD will motivate the users (People) to accept (change their behavior) using the system.
d) Based on a, b, and c, the cues to action as determinants and privacy by design are similar, which is to act dependent on events that motivate the changed behavior. Hence, the cues to action as determinants in this framework were incorporated by adopting a PbD and cues to action. So, the final goal will be achieved, which is preserving PPDP in mobile cloud computing.

In conclusion, the definition of each mentioned facet is clarified as follows:

a) Events = Applying the privacy by design.

b) Motivate = Visibility and transparency in PbD.

c) People = Users.

d) Change their behavior = Accept.

3.5 Conceptual Framework and Hypotheses

In this research, utilizing the proposed framework (A conceptual framework) presented in Figure 3.5 included the following constructs: the perceived benefits, cues to action of PbD, perceived barriers, and perceived threat, which is composed of perceived susceptibility and perceived severity (Koloseni et al., 2019; Edwards, 2015; Orji et al., 2012; Rosenstock, 1974). As shown in Figure 3.6, a total of 6 constructs were utilized. The constructs defined in the proposed framework based on HBM and their related hypotheses are as follows:

(a) ***Privacy and personal data protection behavior in MCC***

Privacy refers to the state of becoming independent of public attention (Jung, 2017; Ranchal et al., 2010). Personal data states any data related to a recognized or identifiable individual (data subject) (Grundstrom et al., 2019; Co-operation & Development, 2002). Behavior is how one acts or mannerisms are made by oneself, particularly towards others (Elizabeth & Lynn, 2014; Cao, 2010). In this study, the behavior is considered in the likelihood of behavior change in HBM. Together, PPDP behavior in the MCC indicates the actions of a country that hosted the actual cloud storage and their behaviors against the violation regarding MCC and malicious behavior.

(b) ***Perceived benefits***

It refers to a change in an individual's behavior when there are perceived benefits in adopting a new activity (Al-diabat, 2019; Rosenstock, 1974). In this context, it refers to

the perceived benefits of location transparency in cloud storage. The main hypothesis articulated in this thesis are as follows:

H1: Perceived benefits are positively related to privacy and personal data protection behavior in mobile cloud computing.

(c) ***Perceived barriers***

It can be acted as a constraint when an individual acts based on the suggested behavior. Although a person may believe that a specific action is decisive in decreasing threats, the activity may result in unnecessary pain or trouble (Koloseni et al., 2019; Vatka, 2019). In this context, mobile cloud computing users perceived the unavailability of location transparency and unsatisfactory data protection laws and regulations. These barriers are likely to reduce privacy performance and data protection behavior in MCC. The following hypothesis is formulated in this thesis:

H2: Perceived barriers are negatively related to privacy and personal data protection behavior in mobile cloud computing.

(d) ***Cues to action of PbD***

Cues to action in the health belief model are events that motivate individuals to change their behavior (Edwards, 2015). According to some researchers, if an individual has been afflicted previously, they might discover upcoming concerns easier (Koloseni et al., 2019; Vatka, 2019; Dodel & Mesch, 2017). The cues to action in this research point directly to the PPDP behavior in MCC as well as directly to the perceived threat to demonstrate if the cues to action influence individual threat perception. This study concerns how location transparency, laws, and regulations act as a protector of PPDP behavior in MCC. It is hypothesized that cues to action will be positively related to the perceived threat. Moreover, it is hypothesized that cues to action will have positively related to privacy and data protection behavior for mobile cloud computing. Therefore, the following hypotheses are formulated in this thesis:

H3: Cues to action of privacy by design, considering visibility location transparency, laws, and regulations are positively related to the perceived threat.

H4: Cues to action of privacy by design, considering visibility location transparency, laws, and regulations are positively related to privacy and personal data protection behavior in mobile cloud computing.

(e) ***Perceived threat***

The perceived threat in the health belief model affects the individual's desire to implement health-related behavior. In addition, it is established by an individual's perceived susceptibility and by an individual's perceived severity of the condition or disease (Young et al., 2016; Edwards, 2015; Glanz et al., 2008). A person may believe vulnerable to a condition or illness but does not think that they are under threat or at risk since they do not think that the illness is severe enough to deal with as a threat. Otherwise, a person might feel that the condition or disease is severe but not feel that they are vulnerable to the illness or condition. Therefore, they don't see it as a threat. Consequently, the conjunction of perceived susceptibility and severity creates a perceived threat (Edwards, 2015).

According to Claar (2011), Ng et al. (2009), and Young (2016), the perceived threat is a mixture of perceived susceptibility and severity. Also, Claar (2011) and Ng et al. (2009) discovered in their studies that perceived susceptibility affects individual's security behavior (Young et al., 2016; Claar, 2011; Ng et al., 2009). Further, Liang et al. (2010) refer to the perceived security threat as the extent to which an individual realizes malicious information technology as harmful or hazardous (Liang & Xue, 2010). Consequently, for this thesis, the subsequent hypothesis is articulated:

H5: Perceived threat is positively related to privacy and personal data protection behavior in mobile cloud computing.

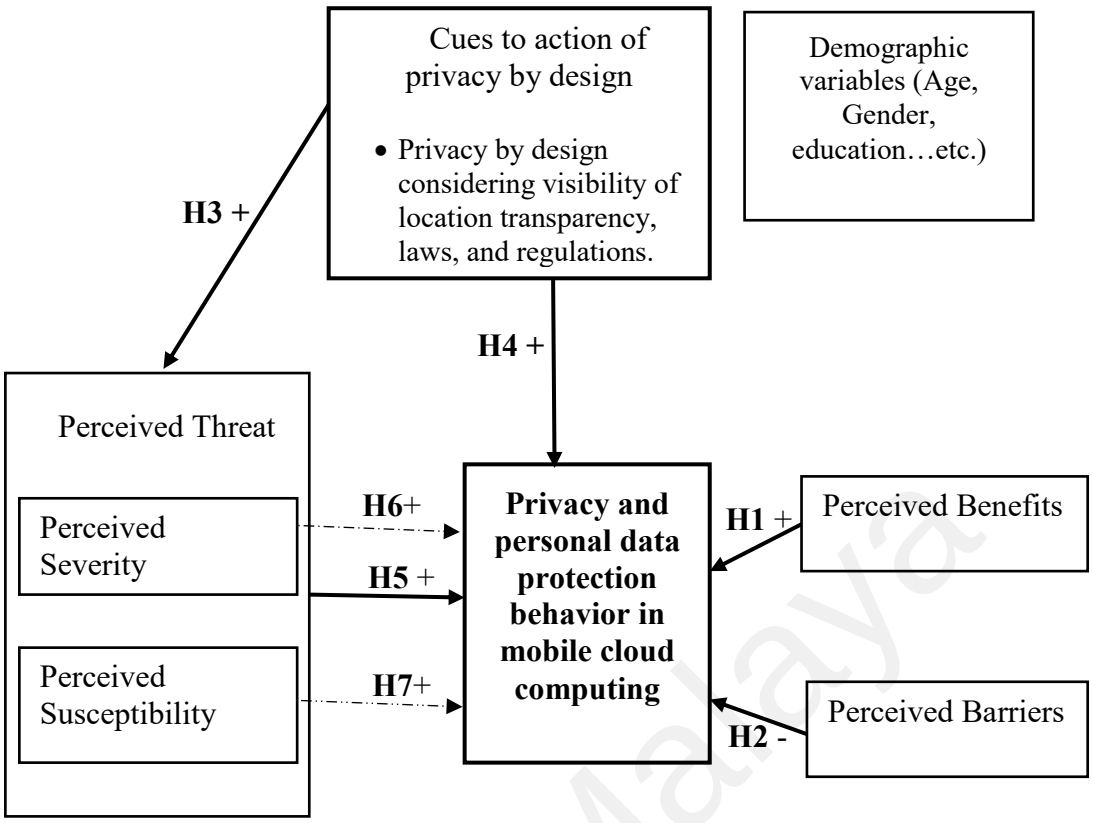
a) Perceived severity: refers to an individual's impression of how the severity of a health situation (Vatka, 2019). In this research, the seriousness or perceived severity is associated with hazards related to some given cloud storage locations, for example, the laws and regulations related to privacy and personal data protection. So, the subsequent hypothesis is articulated in this thesis:

   H6: Perceived severity is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

b) Perceived susceptibility: It handles beliefs or perceived risks of illness development. The individual may be more careful and hence feel worried about the illness. However, the individual may reject the likelihood of developing the illness despite the facts and information about the illness (Al-diabat, 2019; Ng et al., 2009). Accordingly, if mobile cloud computing users notice the significant vulnerability to the violation and threat, one is more likely to take additional precautions to their PPDP behavior in mobile cloud computing. Therefore, for this thesis, the subsequent hypothesis is articulated:

   H7: Perceived susceptibility is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

Figure 3.6 illustrates the proposed PbD framework. The figure shows the relationship between the proposed model constructs regarding PPDP behavior in mobile cloud computing.



Legend	
⟶	Direct Influence.
- - - →	Indirect Influence.
H	Hypothesis.
H+	Positive influence.
H-	Negative influence.

Figure 3.6: Proposed privacy by design framework and hypotheses

3.6 Proposed PbD Framework in the High-Level Architecture of MCC

It is necessary to conduct research on information systems to "further knowledge that aids in the productive application of information technology to human organizations and their management" (Hevner et al., 2004) and to communicate and develop "knowledge concerning both the management of information technology and the use of information technology for managerial and organizational purposes" (Hevner et al., 2004). This knowledge is comprised of three complementary, including design science, behavioral science, and distinct paradigms (Hevner et al., 2004). The behavioral science paradigm evolved from natural science research methodologies. It aims to justify and develop theories (laws and principles) that describe or expect organizational and human

phenomena related to the design, information system analysis, management, implementation, and usage (Hevner et al., 2004).

The design science paradigm has its origin in the sciences and engineering of the artificial (Hevner et al., 2004). It is in fact, a problem-solving paradigm. Further, it aims to develop innovations that describe the products, capabilities, technical practices, and ideas that allow for the effective and efficient analysis, design, management, implementation, and use of information systems (Hevner et al., 2004).

This research proposes the use of privacy by design to preserve privacy and data protection in mobile cloud computing using visibility and transparency, considering location transparency, laws, and regulations. This is to help in selecting the cloud storage, which is hosted in countries that applied laws and regulations for PPDP mobile cloud computing.

The consideration of rigor in design research is based on the researcher's use of relevant theories, intelligent choices, and methods to evaluate and construct the artifact. In addition, Design Science research focuses on current concepts derived from the domain knowledge base (Hevner & Chatterjee, 2010).

The significance of design in IS literature, the related information system research is tied closely to its application in design, and the implications of information systems research should be executable. SO, “As technical knowledge grows, IT is applied to new application areas that were not previously believed to be amenable to IT support" (Hevner et al., 2004).

This study contributes to the enterprise architecture and information systems security in mobile cloud computing by preserving PPDP in the MCC. This research proposes to include allowing the mobile cloud computing user to select a storage location, including the country, cloud storage, and laws and regulations applied. By doing this, visibility of location transparency, laws, and regulations was considered to be implemented. As

displayed in Figure 3.7, the projected PbD framework added to the high-level architecture of MCC in the registration phase and the synchronization phase is as follows:

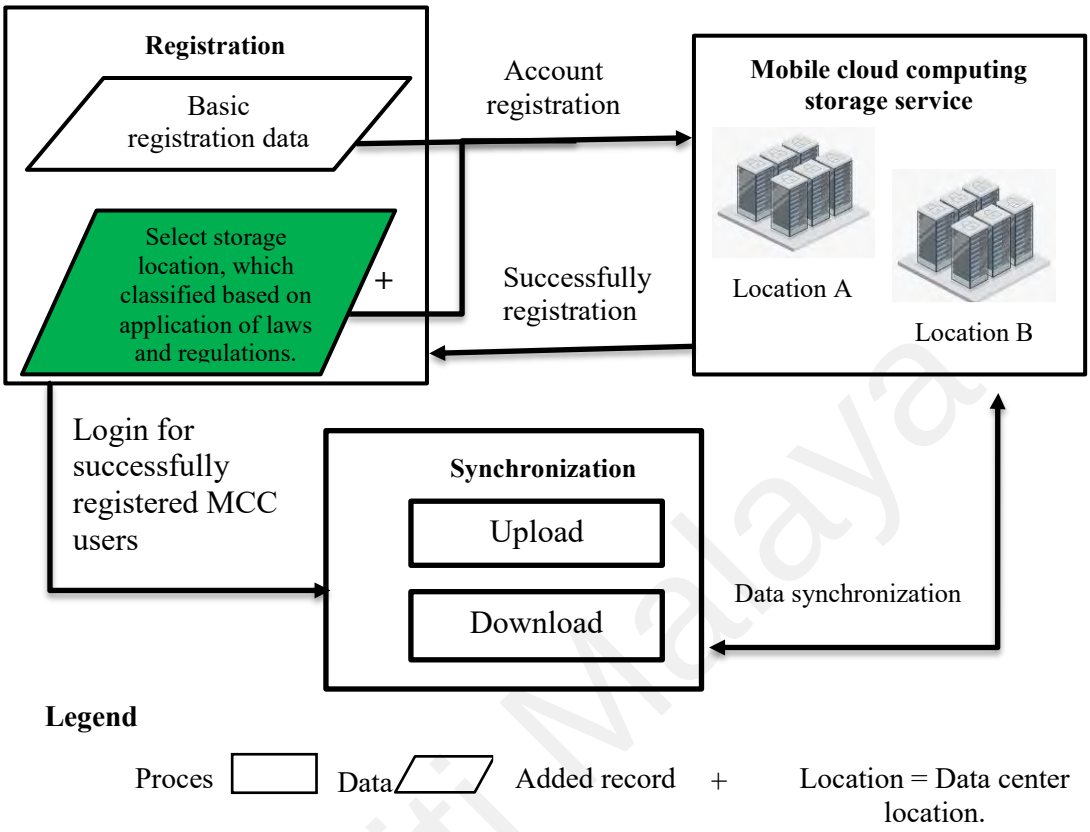


Figure 3.7: Proposed PbD framework in the high-level architecture of MCC

(a) ***Registration phase***

In this phase, the mobile cloud computing user must select the storage location that is classified based on the application of laws and regulations in the mobile cloud computing storage service locations.

(b) ***Synchronization phase***

The projected framework uses the existing synchronization process by adding the location, which includes the ability to know the location of the storage that the user is synchronized. In the synchronization phase, personal data on a mobile device are synced to a server that leads to a mobile cloud computing storage service location.

In this research, as shown in Figure 3.7, the green box shows that the selected storage location, which is classified according to the application of laws and regulations, is

contributed by this research in the high-level architecture of MCC, which is lacking in the literature as presented in Chapter 2 (Sub-section 2.1.4, Figure 2.2 and Section 2.6). The green box shows where and how the proposed PbD framework (Figure 3.6) is applied in the high-level architecture of MCC.

3.7 Summary

This chapter shows the theoretical perspective of this research, including the theoretical perspective of PPDP in the MCC and theories used in information systems security and privacy such as the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Health Belief Model (HBM)., and Theory of Planned Behavior (TPB). Also, this chapter has shown more details about the HBM, including the history of the HBM, HBM assumptions, HBM components, and HBM concepts. Moreover, this chapter has shown a comparative analysis of theories and models, determinants of preserving privacy and personal data protection, and conceptual framework and hypotheses. The next chapter illustrates the research methodology.

CHAPTER 4: RESEARCH METHODOLOGY

This chapter presents the research process, including Literature analysis, privacy by design framework, development of the survey instrument, instrument, validity and reliability, data collection and analyses, SmartPLS, measurement model, and structural model. Finally, a summary of the research methodology is highlighted at the end of the chapter.

4.1 Research Process

In this research, three phases have been used to guide this study, as shown in Figure 4.1. The first phase is the literature analysis through which RO1 and RO2 were achieved. For the RO1, a systematic mapping study (SMS) using quantitative data was conducted, and the output of this investigation was based on the list of current data privacy threats and solutions proposed in the MCC. Also, in Phase 1, a systematic literature review (SLR) and a comparative analysis were conducted to determine the determinants that influence the preservation of PPDP in the MCC. As a result, the privacy by design framework is proposed.

In phase 2, to develop the PbD framework, hypotheses were articulated. Also, a survey instrument was developed and applied, where 386 replies were utilized to test the hypotheses. As mentioned in Section 3.6, this research followed a problem-solving paradigm that aims to develop innovations that describe the products, capabilities, technical practices, and ideas that allow for the effective and efficient analysis, design, management, implementation, and use of information systems (Hevner et al., 2004). Moreover, this research used the Design Science research that focuses on current concepts derived from the domain knowledge base (Hevner & Chatterjee, 2010). In this research, a quantitative analysis was performed on the SEM-PLS based data analyses and the output is the PbD framework. Phase 3 focused on the validation of the PbD framework.

However, to validate the PbD framework, a quantitative methodology is applied using SEM-PLS model fit, and the output validates the PbD framework.

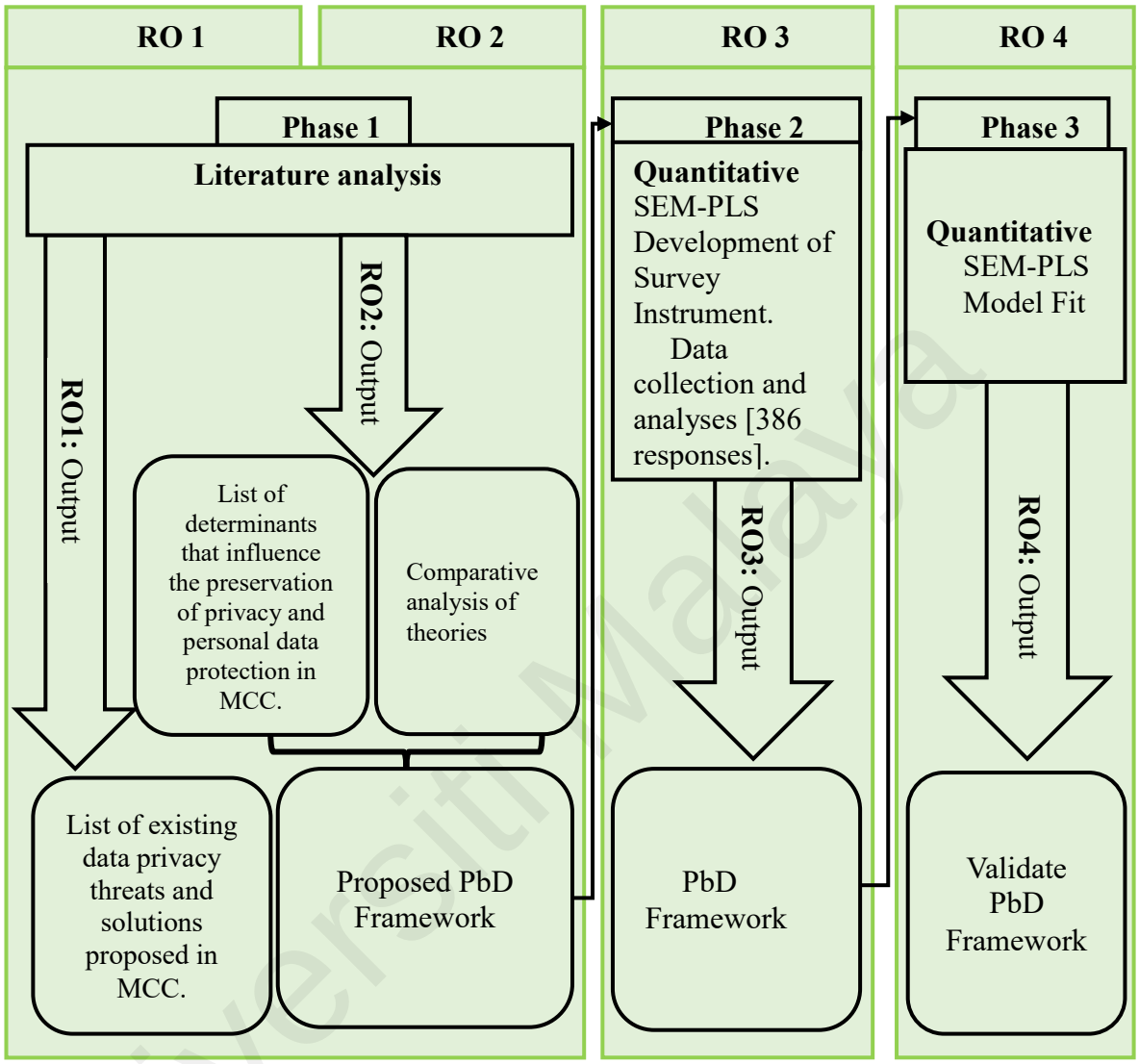


Figure 4.1: Research methodology

4.2 Literature Analysis

In the Literature Analysis of this study, a systematic review is conducted, including a systematic mapping study (SMS) and a systematic literature review (SLR) (Ahmed et al., 2020). The SMS is conducted to identify current threats and attacks on data privacy, and privacy solutions proposed to preserve PPDP in the MCC. Moreover, the SMS method is presented in Sub-section 4.2.1. Furthermore, the SLR is applied to determine the

determinants that influence the preservation of PPDP in the MCC. In addition, the SLR method is presented in Sub-section 4.2.2.

4.2.1 Systematic Mapping Study (SMS) on Privacy and Data Protection in MCC

Currently, several surveys and reviews have been published to investigate mobile cloud computing (MCC) in secondary research (Bhatia & Verma, 2017; David et al., 2017; Kulkarni et al., 2016; Rahimi et al., 2014) and are considered connected with this research. Research in 2017 concentrated on the numerous encryption methods that are currently being used and potential upcoming works that could advance privacy-oriented security and encryption methods (David et al., 2017). Furthermore, the authors attempted to give the audience an idea of the strain of the procedure being used in each of the considered encryption methods (David et al., 2017). Though, they did not discuss other solutions to the current attacks and threats associated with mobile cloud computing (David et al., 2017).

Another study centered on the current mobile cloud computing frameworks, with no further solutions presented (Kulkarni et al., 2016). Moreover, a study offered a state-of-the-art organization of data security strategies as well as advanced delimitation of the chronological sequence using cryptographic approaches (Bhatia & Verma, 2017). Nevertheless, the survey concentrated on threats and attacks linked to the mobile cloud. In addition, Rahimi et al. (2014) conducted several studies on the mobile cloud computing environment, however, most security frameworks for mobile cloud computing shift processor-intensive tasks to the cloud. The study recommended some challenges, such as service providers' requirement to handle and fulfill the privacy and security in mobile cloud computing (Rahimi et al., 2014). Lastly, despite several surveys and reviews stated, two restrictions were identified, which are as follows:

a) There is a necessity for an additional systematic technique in briefing the existing knowledge in mobile cloud computing. The popularity of these studies can be

identified as the fact that they are informal literature surveys that do not involve exact study questions, processor data extractions, determined data analyses, or search methods.

b) While apps on these stands continue to develop, a few secondary research concentrated on PPDP in the MCC.

A Systematic mapping study (SMS) is a secondary data analysis study that delivers a structure for many papers and collects the outcomes announced in the field. Moreover, an SMS is a strategy for classifying published research, providing a visual summary, along with mapping the outcome is utilized to emphasize the latest state of the art and define trends (Witti & Konstantas, 2018). SMS is an extensive examination of primary studies in a particular research field to determine the existing evidence in that field. The majority of the previous studies have implemented systematic mapping studies to aggregate and collect existing evidence in the study field. Accordingly, the SMS has been chosen to perform a thorough analysis of primary studies in a specific study domain to determine available evidence of PPDP in the MCC (Kosar et al., 2016; Kitchenham & Charters, 2007).

In this study, the authors have concluded the formal criteria of a systematic mapping study from Petersen et al.(Witti & Konstantas, 2018).

4.2.1.1 Systematic mapping study process

As in the directive of SMS (Witti & Konstantas, 2018), SMS is accomplished in five phases, with the results of each phase providing input for the next phase. Figure 4.2 illustrates the SMS process, as confirmed in Petersen et al. (Witti & Konstantas, 2018). As shown in Figure 4.2, SMS is implemented as follows (Witti & Konstantas, 2018):

a) Phase one: Describe research objectives and questions to afford a general scope.

b) Phase two: Describe the search method to find the studies in digital libraries.

c) Phase three: The screening process that uses the exclusion and inclusion criteria to select related papers.

d) Phase four: Keywording to data extraction and allowing classification.

e) Phase five: The data extraction and mapping process.

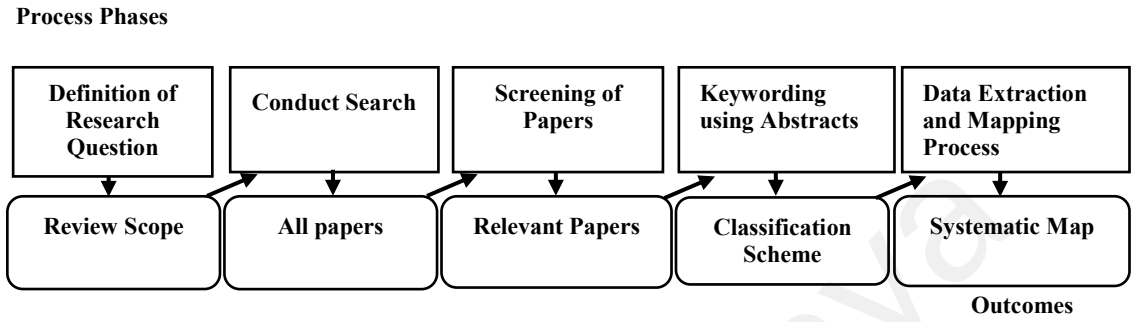


Figure 4.2: The process steps of systematic mapping (Witti & Konstantas, 2018)

(a) ***SMS study questions and objectives***

The researcher conducted an SMS to present the outcomes of current primary studies in privacy and data protection in mobile cloud computing, as well as determining the existing open issues and trends in the area.

(b) ***SMS search strategy***

As in the Systematic mapping study guideline, primary studies are determined via a search string obtained from research questions (Petersen et al., 2008). A powerful technique for structuring a search string is to use PICO (population, intervention, comparison, and outcome) (Petersen et al., 2008). PICO is applied as follows:

a) The population refers to the published studies.

b) The interventions are data protection, MCC, mobile cloud computing, and privacy.

c) The Comparison is not applicable.

d) The Outcome is published research in privacy and data protection in the MCC.

The authors constructed a search string based on PICO, as shown in Figure 4.3. As shown in Figure 4.3, the PICO criteria is used to construct the research string. In this

systematic mapping study, the search string presented in Figure 4.3 is used to search for relevant articles.

("Privacy" OR "data protection") AND ("mobile cloud computing" OR "MCC").

Figure 4.3: Constructed search string for SMS using PICO criteria

Table 4.1: Exclusion and inclusion criteria

Inclusion criteria	**Exclusion criteria**
The selected primary study must be a) Related to MCC. b) Published from 2009 to 2019. c) Present with validation or verification as a contribution related to the domain. d) Peer-reviewed articles only. e) Articles that are written in the English language**.**	The study is: a) Presenting a summary of a keynote, a workshop introduction, or only an abstract. b) Presenting other issues.

(c) ***Exclusion and inclusion criteria***

According to SMS guidelines (Petersen et al., 2008), applying exclusion and inclusion criteria is important to filter the outcomes (Petersen et al., 2008). Exclusion and inclusion criteria determine relevant primary studies by answering defined research questions (Petersen et al., 2008). Table 4.1 illustrates the exclusion and inclusion criteria.

(d) ***Keywording and classification for data extraction***

For the systematic mapping study classification and the data extraction, the conducted SMS (Fatima & Colomo-Palacios, 2018) announced:

a) Classification scheme: This is a review of the abstracts to search for concepts and keywords that reveal the study's contribution (Petersen et al., 2008). It seeks to ensure that the targeted outcomes are achieved in the systematic mapping study (Fatima & Colomo-Palacios, 2018). It also helps in presenting categories that show the principal population (Fatima & Colomo-Palacios, 2018), which makes a high-level comprehension of the contribution and nature of the primary studies selected (Petersen et al., 2008).

b) Keywording: is used to apply the classification scheme in a systematic mapping study as follows. Firstly, read abstracts to search for the keywords (Fatima & Colomo-Palacios, 2018). Secondly, to determine the context connected to the study objective while the scheme is modified (Fatima & Colomo-Palacios, 2018).

c) Scheme: When a categorization scheme is in place, relevant articles are classified into the scheme, i.e., the actual data extraction occurs (Petersen et al., 2008).

As presented in Figure 4.4, the classification scheme is applied as presented below:

1) Keywording: This is the process of reading the abstract to search for keywords, which is used to determine the context connected to the objective of the systematic mapping study (Fatima & Colomo-Palacios, 2018).
2) Sort Article in the scheme: This is a process of sorting the scheme after including a paper in the scheme (Fatima & Colomo-Palacios, 2018).
3) Update scheme: This is the process of adjusting the scheme after including a study context (Fatima & Colomo-Palacios, 2018).

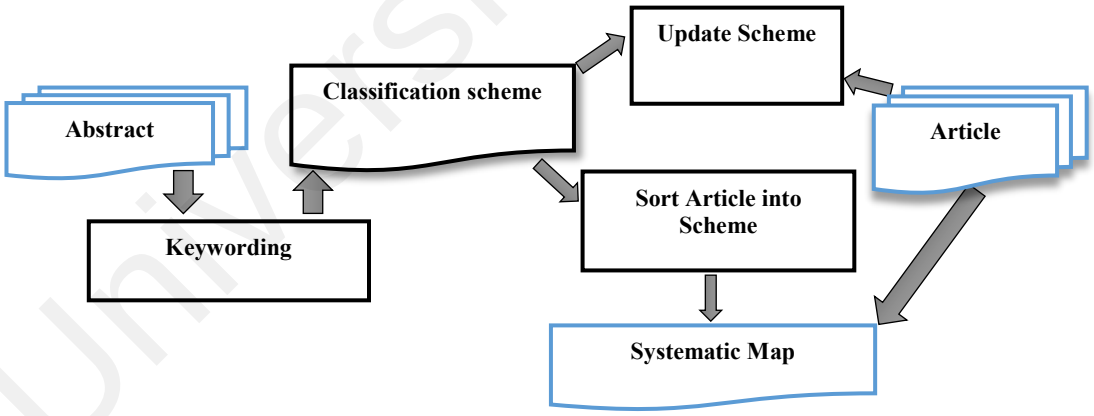


Figure 4.4: Classification Scheme (Fatima & Colomo-Palacios, 2018)

(e) ***Data extraction and mapping process***

As illustrated in the process of SMS (Petersen et al., 2008), in this research, a data extraction procedure is utilized to collect the systematic mapping study data. Also, after a classification scheme is applied, data extraction from related papers linked to publications is sorted according to the subsequent scheme.

a) Excel tables are used to register the process of data extraction (Petersen et al., 2008).
b) The frequencies of articles in the categories are analyzed from a final table (Petersen et al., 2008).

To examine the trends as in the SMS method, (Petersen et al., 2008), the authors concentrated on the rates of papers for the categories to determine which category has been highlighted in previous studies to determine gaps and to detect future studies possibilities. In addition, various ways of analyzing and presenting the outcomes were applied:

a) A summary of statistics is displayed in tables, which show the frequency of papers (Petersen et al., 2008).
b) A Bubble plot displays the frequencies (Petersen et al., 2008). The Bubble plot consists of two x-y scatterplots with a group of bubbles in the category intersections. The bubble's size is proportional to the number of papers that match its coordinates (Petersen et al., 2008).

4.2.1.2 Conducting a systematic mapping study

In this section, the authors present the SMS method that they have conducted in this section. SMS involved two steps: Step A, which is selecting and filtering relevant studies, and Step B, which is the analysis and classification.

(a) ***Selecting and filtering relevant studies***

In this investigation, the research group (three researchers) implemented PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines (Felix & Lee, 2019) as an evidence-based method for showing the result of the search outcomes to elucidate the eligible primary studies included and excluded. PRISMA guideline is used to assess the selection and filtering in the relevant studies. Figure 4.5 determines the resulting papers from each database using PRISMA.

According to Figure 4.5, five digital databases were selected in this study, including Science Direct, ACM Digital Library, Springer Link, IEEE Xplore, and Scopus. For this research, the chosen databases, which contain ACM Digital Library, Science Direct, Scopus, Springer Link, and IEEE Xplore, are a risk to the validity of the systematic mapping study because relevant studies are not included in those selected databases. More importantly, to ease this risk, as pointed out by Dyba et al. (Dyba et al., 2007) and presented by Kitchenham et al. (Kitchenham & Brereton, 2013; Kitchenham & Charters, 2007), the selection of ACM, IEEE Xplore, and any two databases are sufficient to save effort and time in general rather than searching multiple publishers' digital databases (Kitchenham & Brereton, 2013; Dyba et al., 2007). Therefore, in this examination, the researchers have chosen five databases, including ACM and IEEE, which will relieve the risk. Then, the authors used the search string, as shown in Figure 4.5, to search for papers. As an outcome, 1711 studies initially retrieved were screened, as shown below:

a) By article type: Studies offered in magazines, journals, and conference venues were initially selected.
b) By subject: Studies relevant to data protection, privacy, MCC, and mobile cloud computing were initially selected.
c) By title: Relevant to mobile cloud computing was primarily nominated. The title selection is required because the research is focused on mobile cloud computing only.

In summary, after the screening, 215 studies were primarily selected and shown in Table 4.2.

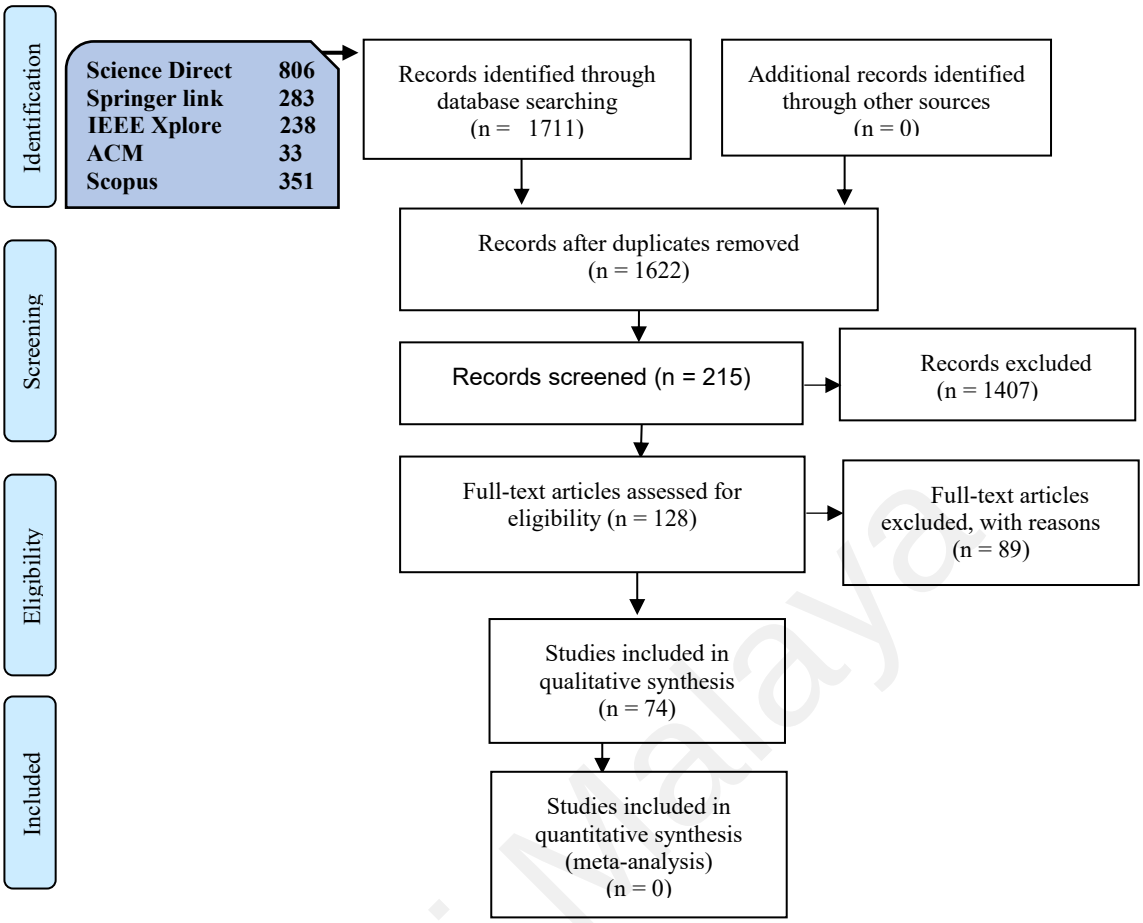


Figure 4.5: PRISMA flow diagram

Table 4.2: The results of the search for relevant studies

Results / Database	Search result	Screen by the last ten years	Screen by article type	Screen by subject	Screen by title
Science Direct	806	693	461	264	78
IEEE Xplore	238	232	227	200	47
Scopus	351	351	290	252	65
Springer link	283	231	93	93	16
ACM	33	23	23	23	9
Total	**1711**	**1530**	**1094**	**832**	**215**

In the filtering of the retrieved studies, 89 papers were excluded using the exclusion and inclusion criteria as shown in Table 4.1. Moreover, 39 studies were removed due to duplication. Furthermore, the authors read 89 studies in the comprehensive analysis. Comprehensive analysis is a procedure of reading a full primary study and deciding whether to exclude or include it after the complete study on the contribution. Finally, 74 primary studies were selected. Table 4.3 displays the outcomes of the filtering process.

Table 4.3: The results of filtering the retrieved studies

Results / Database	Search result.	Comprehensive analysis			Final selection.
		Remaining after inclusion and exclusion.	Remaining after removing duplicated studies.	Remaining after comprehensive analysis.	
Science Direct	78	37	31	31	31
IEEE Xplore	47	27	23	20	20
Scopus	65	46	24	16	16
ACM	9	5	4	4	4
Springer link	16	13	7	3	3
Total	**215**	**128**	**89**	**74**	**74**

*(b) **Analysis and classification***

In this research, the author used keywords to carry out a classification scheme, as declared in Sub-section 4.2.1.1. First, the abstracts of the 74 selected studies were read carefully by looking for keywords. Moreover, the authors read the introduction and conclusion of each chosen study to demonstrate the classification scheme. As a result, the following parts were defined.

a) Data privacy exercises: It refers to approaches of regulatory and application of privacy solutions in MCC (Ahn, 2014). It is concerned with the display of practices and policies for data access utilizing different methods (Blume, 2010) that are regulated by the policies of mobile cloud computing service providers, roles, and state legislation.

b) Attacks and threats: An attack is a breach in system security caused by an intelligent threat. So, this intelligent activity is a suggested attempt (particularly in the concept of a technique or method) to prevent the security services and security policy of the system (Stallings, 2006). A threat is a possible breach of security that arises when there is an occasion, capability, circumstance, or activity that has the potential to do damage and violate security. A threat is a potential hazard that might misuse a vulnerability (Stallings, 2006).

c) Privacy Solutions: These are computational techniques that deals with access control, encryption, authentication, trust, and authorization issues.

The SMS result is presented to answer the RQ1 that concerns the existing privacy threats and existing solutions proposed to preserve PPDP in the MCC (presented in Chapter 2, Section 2.2, and Section 2.3).

4.2.2 A Systematic Literature Review (SLR) on Determinants of Preserving Privacy and Personal Data Protection

For this study, a systematic literature review (SLR) is conducted to provide an answer to RQ 2. The SLR is accompanied by the guidelines presented in the literature (Hussain et al., 2019; Keele, 2007). In other words, the employed SLR helps to determine the determinants that influence the preservation of PPDP in the MCC. Figure 4.6 displays the phases of the SLR. The following paragraphs highlight the conducted SLR.

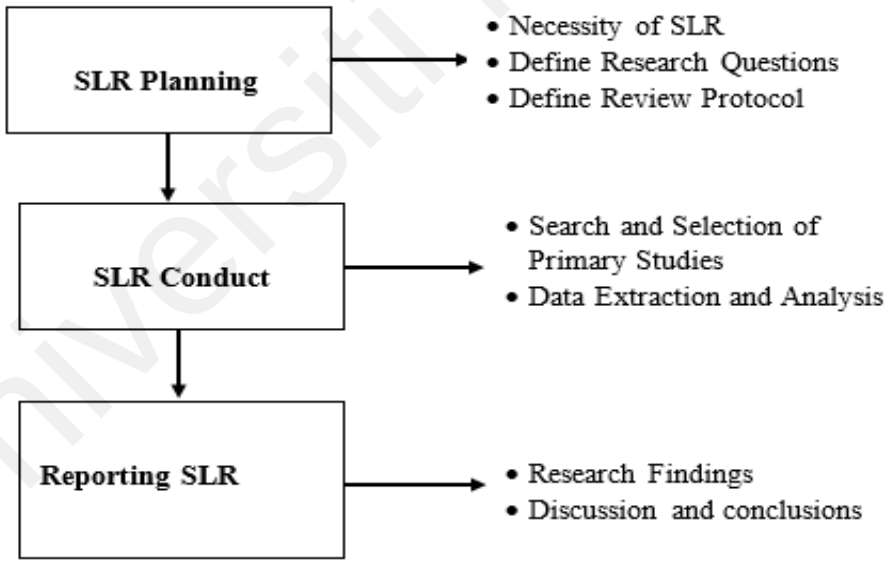


Figure 4.6: SLR process (Hussain et al., 2019)

4.2.2.1 Systematic literature review planning

For this study, a search string is formulated to search for studies in electronic databases. Specifically, five electronic databases were selected, including Springer link, Scopus, Science Direct, ACM, and IEEE Xplore. Precisely, the research string is:

('Preserve' or 'Perceived' and 'privacy' or 'security' and 'information privacy' or 'information security', and 'Theory' and 'Model' or 'framework') OR ('privacy' or 'security; and 'information privacy' or 'information security' and 'Theory' and 'Model' or 'framework'). In detail, a review protocol that includes the primary study selection process, filtering process, and data analysis is applied (Hussain et al., 2019). Moreover, exclusion and inclusion criteria are utilized to select primary studies (Petersen et al., 2008). The following paragraphs show the exclusion and inclusion criteria followed in the SLR.

(a) ***Inclusion criteria***

a) The primary study must be connected to preserve or perceived privacy or security and published from the year 2009 to the year 2019.
b) The primary study must make a contribution that includes verification or validation related to privacy or security.
c) Primary studies were written in the English language.

(b) ***Exclusion criteria***

a) Primary study gives a summary of a workshop introduction, a keynote, or only an abstract.
b) Studies about other issues other than preserve or perceived privacy or security.
c) The primary study does not present a theory and framework or a model to preserve privacy or security.
d) The primary study does not present determinants that preserve privacy or security.

After applying the inclusion and exclusion criteria, a comprehensive analysis is carried out in the SLR. A comprehensive analysis related to the procedure of reading a full primary study to decide if to exclude or include it after a complete investigation of its contribution. It helps in determining the determinants that influence the preservation of PPDP in the MCC.

4.2.2.2 Conducting a systematic literature review

In conducting the SLR, as shown in Figure 4.7, in the primary study selection process (Hussain et al., 2019), 378 primary studies were identified when searching for studies in the selected databases using the search string presented in Sub-section 4.2.2.1. After the filtering process displayed in Figure 4.7, 19 primary studies were selected and investigated to identify determinants that influence the preservation of privacy or security in the literature utilized in this study. Table 3.2 shows the selected primary studies in the SLR and the identified determinants with related theories in the selected primary studies. Results of the SLR are highlighted in Sub-section 3.3.1.

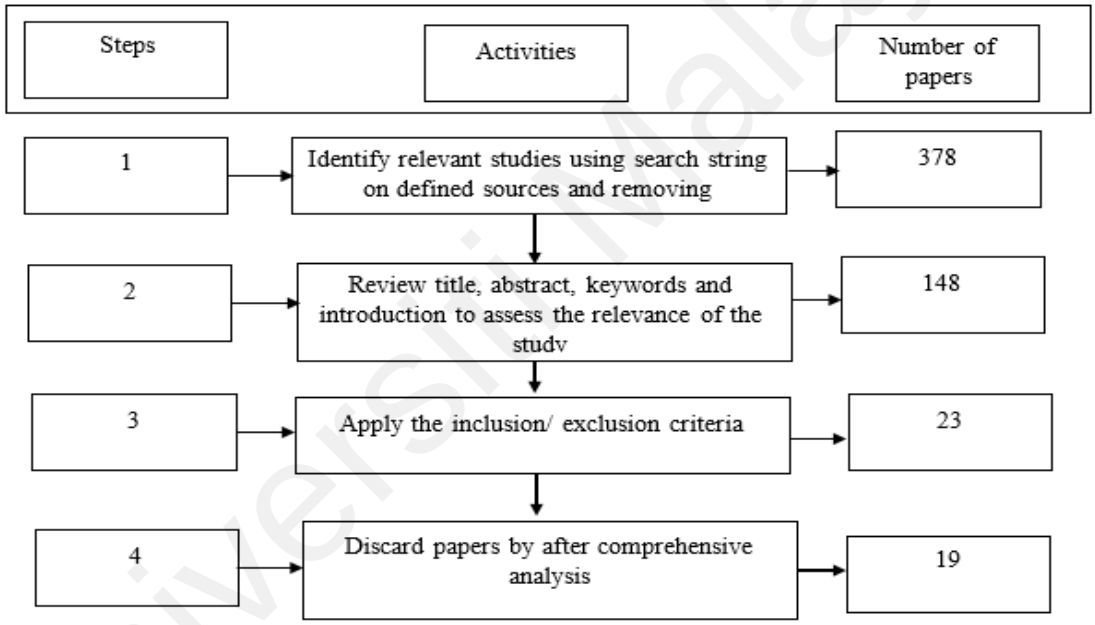


Figure 4.7: Primary studies selection process

4.4 Development of Survey Instrument and Data Collection and Analyses

This section presents the instrument, scale measurement, and Likert scale.

4.4.1 Instrument

The instrument is defined as the measuring tools, such as designed questionnaires, to obtain data on a specific topic, where the researcher is needed to identify the type of tool to be used, based on the type of study the researcher will conduct, which includes qualitative, quantitative, and mixed-method (Wilkinson & Birmingham, 2003).

For example, the researcher may decide to use quantitative research; the questionnaire may be used to do an investigation. The researcher who uses a qualitative study may use a suitable scale. It helps in the creation of the instrument because its efficacy was already created and the researcher can use a new instrument or even build his instrument if needed. The researcher needs to identify the instrument(s) used in the research manuscript in the methods section (Wilkinson & Birmingham, 2003).

As this study concerns visibility and transparency, privacy by design aims to assure all stakeholders that whatever the business practice or technology involved, it works by following the stated goals and it is subject to independent verification. Its constituent parts and processes are visible and transparent to both providers and users.

In this study, the instrumentation is implemented as follows:

A questionnaire has been prepared and presented in Appendix A; the questionnaire is separated into two parts, as presented below:

(a) ***The first part***

The first part contains demographical data, for example, Gender, Age, Marital status, Cloud storage, and education.

(b) ***The second part***

The second part consists of the constructs that were arranged as presented below:

a) Perceived threat consists of two sub-dimensions, counting the perceived severity of risks associated with some given cloud storage locations that do not apply laws and regulations of PPDP and the perceived susceptibility to violation and threat. Perceived susceptibility was evaluated with four items; while perceived severity was evaluated with five items adapted from Al Khater's study and self-developed (Al Khater, 2017).
b) Perceived benefits evaluated with six items developed by Al Khater and self-developed (Al Khater, 2017).

c) Perceived barriers evaluated with items developed by Al Khater and self-developed (Al Khater, 2017).

d) Cues to action of PbD evaluated with six items developed by Al Khater and self-developed (Al Khater, 2017).

e) Privacy and personal data protection (PPDP) behavior in mobile cloud computing evaluated with five items developed by Al Khater and self-developed (Al Khater, 2017).

This research utilized a survey to collect the data from participants, including users who utilized the cloud in MCC to save their data. Also, this study used a survey because the survey method is used to collect information and offers a comprehensive explanation of the beliefs and directions of a specific population by examining a sample of that population (Aityan, 2022). More importantly, this study investigated PPDP in the MCC, which is directly related to individual data, making the survey questionnaire a relevant approach to be used in this study.

4.4.2 Scale Measurement

The scale of measurement is determined by the methods in which variables and numbers are defined and classified (Stevens, 1946). Hair et al. (2017) referred to the scales of measurement as an instrument with a fixed number of shuttered answers that may be utilized to get answers to questions (Hair Jr et al., 2016). Every scale of measurement has certain characteristics that set the suitability for using certain statistical analyses, which can be shared into four scales of measurement, which are interval, ordinal, ratio, and nominal.

a) Nominal scale: It is also referred to as a categorical scale. It measures predict numbers that are utilized to define attributes such as products, occupations, or people. It can determine each category by a certain number pointed to it, as this number can be utilized as the percentage in all categories or the count of the numbers of responses

(Stevens, 1946). For example, if the gender is added as a variable, the Female may be coded as number 1 and Male as number 2 and those numbers of variables can be used to represent the categories of data.

b) Ordinal scale: It is a measure to show a rank order or ordered sequence of relations. The order of value is used to predict what is significant. When using an ordinal scale to measure a variable, the change in the value, whether an increase or decrease in the variables, is predicted if it is significant or not (Hair Jr et al., 2016). This type of measurement enables one who used a survey to place the answers in a continuum with the thought that some categories will override other categories. For illustration, in a question, the answer to it would be a multiple choice. For example, **How do you feel today?** The answers might be:

(1) Very unhappy.

(2) Unhappy.

(3) Ok.

(4) Happy.

(5) Very happy.

In this question, it is well known that #4 is better than #3, #2, and #1, but do not know how better it is. Where the difference between unhappy and ok is the same as happy and very happy, fundamentally, these measures do not represent a measurable quantity (Dawson, 2002). An individual may choose #5 in this question and feel less than someone who chose #1. An individual may not be in half as much feel if they chose #2 instead of #4. The only thing that can be known about responding to #2 is less feeling than the responder to #4 through this data.

c) Interval scale: It is use to predict the delicate information on the scale order in which the quantity of knowledge is measured. However, zero is just a supplementary measurement point, which means zero is not the absolute lowest value. According to

Hair et al., an accurate comparison can be carried out between these scales (Hair Jr et al., 2016). For example, the Fahrenheit scale is a good example of a measured interval scale because the interval data are shown in 50 degrees Fahrenheit or -10 degrees Fahrenheit.

d) Ratio scale: There is no difference between interval and ratio since the ratio has equal units and represents the quantity. The ratio has a zero value but no number below zero. The ratio scale of measurement can be used when scaling, such as time, length, or volume (Hair Jr et al., 2016).

4.4.3 Likert Scale

Rensis created the Likert scale in 1932 to study people's attitudes (Likert, 1932). In addition, the Likert scale was used in this investigation to measure the items. The items are supported by an ordinal and interval scale approach (Chin et al., 2003). The measurement is the 5 points Likert scale in this thesis (Brown, 2010) which includes 5 = strongly disagree, 4 = disagree, 3 = undecided, 2= agree, and 1= strongly agree. Moreover, the Likert scale has been used widely since it was established and has been utilized in several surveys to measure the significance of various attitudes (Koloseni et al., 2019; Vatka, 2019; Dodel & Mesch, 2017; Yahya, 2017; Humaidi & Balakrishnan, 2015; Esmaeili, 2014; Claar, 2011; Ng et al., 2009).

In this study, for all of the determined constructs, the 5-point Likert scale was the measurement followed, including 5 = strongly disagree, 4 = disagree, 3 = undecided, 2 = agree, and 1 = strongly agree (Brown, 2010).

4.5 Instrument Validity and Reliability

In this thesis, the validity and reliability are demonstrated for the questionnaire, pilot study, and main study. First of all, the questionnaire is administered through Google forms, a web-based survey platform, since it is easy for the participant to respond to the

questionnaire (Vasantha & Harinarayana, 2016). To ensure validity and reliability, the researcher has implemented the following:

a) The questionnaire has been sent to experts for validation (Petrić & Czárl, 2003; Wallace et al., 2003). Specifically, a questionnaire is sent to experts for validation in studies that employ questionnaires (Esmaeili, 2014). So, the first initial draft was received by experts, who included two tenure-track academic members from the University of Malaya and one of the MCC security specialists. Table 4.4 displays the list of experts involved in content validation.

Table 4.4: Background of experts involved in content validation

#	Experts	Profession	Background
1	Expt1	Academician	A Ph.D. holder specializing in information systems and an expert in data security (Personal data protection, and information security & privacy) and ICT law (Data protection act).
2	Expt2	Professional Practitioner	A Ph.D. holder in Cloud Security. Has a proven track record of working in the ICT industry and deeply specialized in CC, Cybersecurity, and Big Data. Currently engaged in several consultancies in banking, healthcare, Security, and Defense.
3	Expt3	Academician	A Ph.D. holder specializing in information systems and an expert in E-Government, ICT Policies (ICT policies, ICT security, ICT audit, ICT governance), and quantitative data analysis.

b) In the expert validation, the experts comprehensively revised the survey questionnaire, considering all constructs and intended measurement items in detail. They also exerted their effort to simplify the questionnaire and take care of the construction and simplification of the questions to be understood by the respondents. As a result, the expert's validation has validated and improved the survey questionnaire.

c) Pilot study: In this research, the researcher conducted the pilot study by sending the questionnaire to the response using LinkedIn and Facebook. In the pilot study, the

questionnaire was circulated to a hundred respondents who utilized the mobile cloud computing service and who did not take part in the main research. Also, in the research project, the pilot test is considered one of the most important phases and aims to determine possible problem areas in addition to weaknesses in the research instrument in a small group of participants to validate the model quantitatively before distributing the large study to the participants. Hassan et al. (2006) defined the pilot test as a small test that is used to test the research methods, instruments of data collection, sample recruitment approaches, and other techniques to prepare the main study. The pilot study lasted a month, and one of the most difficult challenges for the researcher was searching for participants and their willingness to participate. In addition, the participants had to be reminded from time to time to respond to the questionnaire due to their preoccupation with their daily work responsibilities.

d) As suggested by (Yacob et al., 2017; Taherdoost, 2016; Bagozzi & Yi, 1988), all reflecting indicator loadings overtook the acceptable value of 0.60. Furthermore, loading items with a threshold value of 0.50 are valid (Shah, 2019; Hair, 2009). In the result of the pilot study, the loadings of all reflective indicators exceeded the required cut-off level of 0.60 as recommended by Yacob et al. (2017) and Bagozzi and Yi (1988), except for three questions that were excluded. Moreover, the majority of respondents (69%) have stored their data on Google drive. Respondents' ages range from 30 – 39 years of age (41%).
e) The questionnaire was adjusted based on the outcomes of the pilot test and sent again to experts.

4.6 Data Collection and Data Analyses

After proving the validity and the reliability of the questionnaire, the questionnaire was circulated for data collection as follows:

a) The questionnaire is administered through Google forms, a web-based survey platform since the web-based survey is easy for the participant to respond to the questionnaire (Wohlin et al., 2012).
b) There was a cover letter to show the research purpose to the respondents. It was made clear to the participants that the purpose of the questionnaire was only for the study and not for other purposes, as they agreed to participate.
c) An electronic link is created for the survey and sent to the respondents.
d) In this study, no personal data collected from respondents was used to protect their privacy.
e) The questionnaire was circulated and shared via social media platforms such as LinkedIn and Facebook.
f) The questionnaire link was shared on Facebook with over 550 respondents and over 600 LinkedIn contacts. Purposive sampling was used (Tongco, 2007; Tumusiime, 2004). The participants of the questionnaire of this study are public MCC users around the world, which comprised users who use cloud platforms in mobile cloud computing to store their data, including Google Drive, iCloud, Dropbox, and One Drive (formerly Sky Drive), or others.

As an outcome, 386 responses were received to justify the nature and suitability of the sample group from which the 386 responses have been derived. Hair et al. (2006) proposed sample size of 100-150 for the main study and the model comprises seven or fewer constructs. Moreover, Creswell (2012) recommended that a survey has a minimum sample size of 350 responses to be valid (Creswell, 2012). Accordingly, the sample size for this study is 386 participants, which is considered adequate (Creswell, 2012; Hair et al., 2011; Hair et al., 2006). More importantly, those 386 responses are coming from individuals who used MCC, and in the cloud, who used Google Drive, iCloud, Dropbox, One Drive (formerly Sky Drive), or others.

For the data transfer, the researcher has implemented as presented below:

a) The data was collected from the online tool. Since all the questions in the survey questionnaire are mandatory, the unfinished survey is automatically not allowed to continue. So, the sample of 386 responses completed the answers to all the questions.

b) The transfer of the data was implemented via intermediary software, namely Microsoft Excel, to clean the data, which transfers the data file to a computer database. Also, the excel file was saved as a Comma-Separated Values (.csv) file to make it compatible with the SmartPLS software.

c) The data was imported into SmartPLS software through a Comma-Separated Values (.csv) file. Figure 4.8 illustrates the data collection and analysis processes.

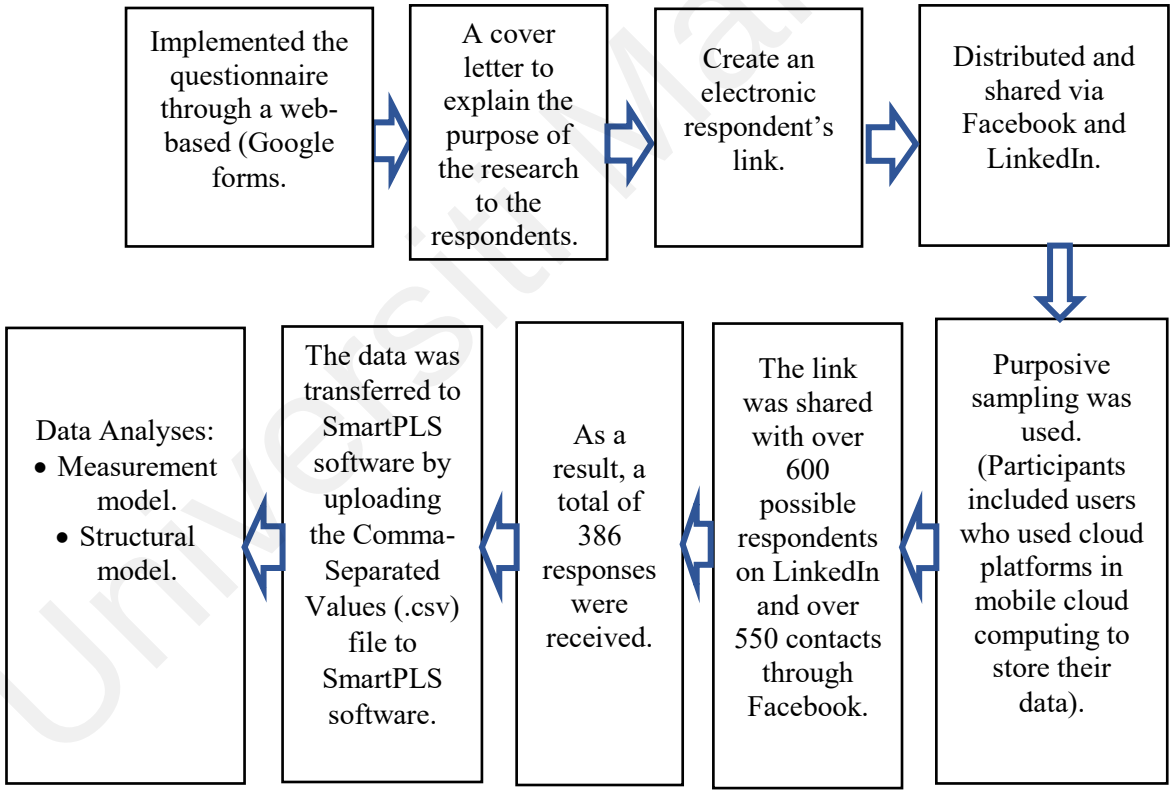


Figure 4.8: The process of data collection and data analysis

4.7 SmartPLS

Structural Equation Modeling (SEM) was utilized in this study, specifically SmartPLS, to test hypotheses. Gefen et al. (2000) indicated that SEM could be used to calculate and

analyze casual relations and qualitative. In addition, the main strength of SEM is the building of latent variables (Gefen et al., 2000).

For latent variables analysis, the SmartPLS uses the Partial Least Squares (PLS) met hod. The SmartPLS is one of the distinguished software implementations for Partial Least Squares Structural Equation Modeling (PLS-SEM). In 2005 the SmartPLS was established by Ringle et al., and the software has advanced reporting features and a friendly user interface; because of that, the software gained popularity since it started in 2005 (Wong, 2013). A SmartPLS software can be utilized to test the factors loading, reliability testing, and construct the path coefficient table, including visualizing the latent variables and T-test values. Furthermore, to examine the significance of both the external and internal model, SmartPLS calculates the T-statistics using a procedure named bootstrapping (Esmaeili, 2014).

The SmartPLS can generate two main models and recognize them.

a) Measurement model: In SmartPLS software, under the calculate list, it can be found that the bootstrapping that can measure the items loading within each construct is given by t-values, which are utilized to check the importance of each question (Chin, 1998b). For these reasons, the measuring model was used along with bootstrapping to test the construct validity (Esmaeili, 2014).
b) Structural model: It can be utilized to test the hypothesis, where SmartPLS calculates the R^2 and path coefficient (Esmaeili, 2014).

4.8 Measurement Model and Structural Model

Overall, the SmartPLS is used to generate two main models (Esmaeili, 2014), the measurement model and the structural model, which are clarified as keen below.

4.8.1 Measurement Model

The measurement model comprises relationships between their indicators (items) and the latent variables (Williams et al., 2014). It can be used to determine the items loading,

and for checking the importance of each question inside constructs using t-values. However, bootstrapping is under the calculated list (Esmaeili, 2014; Chin, 1998a). Also, the convergent validity, reliability, and discriminant validity (Williams et al., 2014) are measured using the SmartPLS (Ab Hamid et al., 2017; Williams et al., 2014; Fornell & Larcker, 1981).

4.8.1.1 Convergent validity and reliability

According to Hair et al. (2011), convergent validity is identified as the internal consistency scale (Fornell & Larcker, 1981). Besides, the variance inflation factor (VIF) is utilized to assess multi-collinearity (Williams et al., 2014). Overall, convergent validity is measured by the average variance extracted (AVE) (Ab Hamid et al., 2017). The reliability is measured by composite reliability (CR) (Ab Hamid et al., 2017) and Cronbach's alpha (CA) (Ab Hamid et al., 2017).

a) The average variance extracted (AVE): The internal consistency of the construct is assessed by using the AVE test, according to Fornell and Larcker (1981), which can measure the amount of variation a latent variable obtains from its measuring items related to the amount of variance caused to measuring errors (Hair Jr et al., 2017; Fornell & Larcker, 1981). Furthermore, the main assumption for AVE is to be positive, and AVE should be higher than 0.5 (Shmueli et al., 2019; Hair Jr et al., 2017; Fornell & Larcker, 1981).

b) Composite reliability (CR): It is a measure that can be utilized to assess how effectively the allocated indicators measure a concept (Hulland, 1999). In addition, there is a similarity between it and Cronbach's alpha. Also, according to Fornell and Larcker (1981), the score of composite reliability of internal consistency is superior to Cronbach's Alpha measure since composite reliability uses item loadings gained within the theoretical model (Shmueli et al., 2019; Fornell & Larcker, 1981).

c) Cronbach's alpha (CA): It is the data utilized to measure reliability or consistency. Also, Cronbach's Alpha weighs all items identically, regardless of their factor loadings (Hulland, 1999). In addition, Litwin (1995) recommended that the value of CA should be greater than 0.7, while Churchill (1979) and Chin (1998) suggested that it is acceptable to take the internal consistency of Cronbach's alpha value with 0.6 (Sarstedt et al., 2017; Chin, 1998b; Litwin, 1995; Churchill Jr, 1979).

d) The variance inflation factor (VIF) is employed to assess multi-collinearity (Scott, 2020; Williams et al., 2014).

4.8.1.2 Discriminant validity

According to a study, discriminant validity indicates the degree to which the measurements of various constructs differ from each other. Cross-loadings of the model's essential measurement items, the Fornell-Larcker criterion, are used to assess discriminant validity (Fornell & Larcker, 1981), and the Heterotrait-Monotrait Ratio (HTMT) (Henseler et al., 2015) are as follows:

a) Cross loadings: It is an approach utilized to evaluate the discriminant validity in which the factor loading indications on the allocated construct must be greater than the total loading of all other constructs (Ab Hamid et al., 2017; Hair Jr et al., 2016).

b) Fornell-Larcker criterion: It is a method utilized to evaluate the discriminant validity by comparing the correlations among latent constructs with the square root of the average variance extracted, in which a latent construct is required to be higher on its indicator rather than the variance of other latent constructs (Ab Hamid et al., 2017; Hair Jr et al., 2016).

c) Heterotrait-Monotrait Ratio (HTMT): Henseler et al. (2015) proposed a method that tested the Heterotrait-Monotrait Ratio (HTMT) of the correlations to examine the discriminant validity (Henseler et al., 2015). The HTMT method illustrated how the

actual correlation between the two latent variables can be estimated (Ab Hamid et al., 2017; Henseler et al., 2015).

For instance, Table 4.5 offers a summary of assessments of reflective measurement models.

Table 4.5: Assessment of reflective measurement models

Validity Type	Criterion	Guideline	References
Internal Consistency reliability	Composite reliability (CR)	CR > 0.7 or higher.	(Shmueli et al., 2019; Joe F Hair Jr et al., 2017; Sarstedt et al., 2017; Hulland, 1999; Fornell & Larcker, 1981).
Internal consistency reliability	Cronbach's alpha (CA)	CA higher than 0.70.	(Shmueli et al., 2019; Joe F Hair Jr et al., 2017; Sarstedt et al., 2017; W. W. Chin, 1998b; Litwin, 1995; Churchill Jr, 1979).
Indicator Reliability	Indicators/ Outer loadings	0.70 Or higher is preferred. If it is exploratory research, 0.4 or higher is acceptable.	(Kamis, 2021; Chua, 2018; Joseph F Hair et al., 2006).
Convergent validity	AVE	It should be 0.5 or higher.	(Shmueli et al., 2019; Joe F Hair Jr et al., 2017; Joe F Hair et al., 2011; Hulland, 1999; Fornell & Larcker, 1981).
Discriminant validity	Cross-loadings	Each measurement item should have higher loading on its own key construct than any other key construct.	(Ab Hamid et al., 2017; Joseph F Hair Jr et al., 2016; Ringle et al., 2015).
Discriminant validity	Fornell-Larcker criterion	The values of the key construct higher on themselves than other constructs.	(Al-Maroof & Al-Emran, 2018; Ab Hamid et al., 2017; Joseph F Hair Jr et al., 2016).
Discriminant validity	Heterotrait-Monotrait Ratio (HTMT)	HTMT of 0.85 (Stringent Criterion) HTMT of 0.90 (conservative criterion).	(Al-Maroof & Al-Emran, 2018; Ab Hamid et al., 2017; Henseler et al., 2015).

As illustrated in Table 4.5, the assessment of the reflective measurement model is applied in the literature using internal consistency reliability (Shmueli et al., 2019; Hair Jr et al., 2017), indicator reliability (Kamis, 2021; Chua, 2018; Hair et al., 2006), convergent validity (Shmueli et al., 2019; Hair Jr et al., 2017; Fornell & Larcker, 1981), and discriminant validity (Ab Hamid et al., 2017; Hair Jr et al., 2016; Ringle et al., 2015).

As displayed in Table 4.5, in measuring the internal consistency reliability, composite reliability (CR) (Shmueli et al., 2019; Hair Jr et al., 2017; Sarstedt et al., 2017) and Cronbach's alpha (CA) (Shmueli et al., 2019; Hair Jr et al., 2017; Sarstedt et al., 2017) is used in this research.

Moreover, as shown in Table 4.5, the indicator reliability is measured in this research using indicator loadings (Kamis, 2021; Chua, 2018; Hair et al., 2006). On the other hand, the convergent validity is measured in this research by utilizing the average variance extracted (AVE) (Shmueli et al., 2019; Hair Jr et al., 2017; Fornell & Larcker, 1981). Furthermore, the discriminant validity is measured in the literature using cross-loadings (Ab Hamid et al., 2017; Hair Jr et al., 2016; Ringle et al., 2015), Fornell-Larcker criterion (Al-Maroof & Al-Emran, 2018; Ab Hamid et al., 2017; Hair Jr et al., 2016), and Heterotrait-Monotrait Ratio (HTMT) (Al-Maroof & Al-Emran, 2018; Ab Hamid et al., 2017; Henseler et al., 2015).

4.8.2 Structural Model

The structural model is employed to test the hypothesis, and SmartPLS is used to obtain the path coefficient for each hypothesis, Coefficient of determination (R-squared), and effect size (Esmaeili, 2014). In general, the path coefficient contains the T-test values and latent variables (Esmaeili, 2014). R-squared (R^2) values of the endogenous variables are used to determine the standard path coefficient of each relevant endogenous and exogenous variable and to measure the predictive capacity of a particular model or construct (Janadari et al., 2016). Also, the effect size is a statistics term that measures the

correlation strength among two variables on a numerical scale (Cohen, 1988). Effect size (f^2) is used for assessing the effects of particular exogenous constructs on the endogenous construct.

For clarification, to validate the PbD framework, model fit analysis has been used, including Lateral Collinearity, Path Coefficient, Coefficient of determination (R^2), Predictive Relevance (Q^2), Effect Size (f^2), and Goodness of Fit (GOF) measures (Yap, 2022; Adjei et al., 2021; A. A. Ikram et al., 2021). For description, Table 4.6 offers a summary of the assessment of the structural model.

Table 4.6: Assessment of the structural models

Validity Type	Criterion	Guideline	References
Model validity	Coefficient of determination (R^2)	0.75 – Substantial. 0.50 – Moderate. 0.25 – Week.	(Kassem et al., 2020; Scott, 2020; Joseph F Hair Jr et al., 2016; Falk & Miller, 1992).
Model validity	Path coefficients	P value <0.05.	(Xhafaj et al., 2021; Scott, 2020; Joseph F Hair Jr et al., 2016).
Model validity	Predictive relevance (Q^2)	$Q^2 > 0$ (Predictive Relevance). $Q^2 < 0$ (Lacks of predictive Relevance).	(Kassem et al., 2020; Scott, 2020; Joseph F Hair Jr et al., 2016)
Model validity	Effect Size (f^2)	Value of 0.35 large. Value of 0.15 medium. Value of 0.02 Small. Value of 0.01 very small.	(Scott, 2020; Hosseini et al., 2018; Abd Razak et al., 2016; Sawilowsky, 2009).
Model validity	Goodness of Fit (GOF)	GoF is less than 0.1 (no fit.) GoF between 0.1 to 0.25(small). GoF between 0.25 to 0.36 (medium). GoF greater than 0.36 (large).	(Adjei et al., 2021; Azizah & Puspito, 2021; A. Ikram et al., 2021; Kassem et al., 2020; Scott, 2020; Akter et al., 2011; Wetzels et al., 2009; Ali et al.).

As shown in Table 4.6, an assessment of the structural models is applied in the literature using model validity measures (Adjei et al., 2021; Azizah & Puspito, 2021; A.

Ikram et al., 2021; Kassem et al., 2020; Scott, 2020; Hair Jr et al., 2016; Akter et al., 2011; Sawilowsky, 2009; Wetzels et al., 2009; Ali et al.).

For clarification, as shown in Table 4.6, the model validity of this research is measured by utilizing the coefficient of determination (R^2) (Kassem et al., 2020; Scott, 2020; Hair Jr et al., 2016) as well as path coefficients (Xhafaj et al., 2021; Scott, 2020; Hair Jr et al., 2016). Furthermore, the model validity in the literature is also measured using effect size (f^2) (Scott, 2020; Hosseini et al., 2018; Abd Razak et al., 2016; Sawilowsky, 2009), predictive relevance (Q^2) (Kassem et al., 2020; Scott, 2020; Hair Jr et al., 2016), and Goodness of Fit (GOF) (Adjei et al., 2021; A. Ikram et al., 2021; Scott, 2020).

4.9 Summary

This chapter (Chapter 4) presents the research methodology that is used to examine and explain the outcome of the research questions. In summary, three phases are used to guide this study to achieve the research objectives (ROs). The first phase is the Literature Analysis through which RO1 and RO2 were achieved. For the RO1, a Systematic mapping study (SMS) was conducted using quantitative data, and the output of this investigation was a list of current data privacy threats and solutions proposed in the MCC. Also, in Phase 1, a systematic literature review (SLR) was conducted to determine the determinants that influence the preservation of PPDP in the MCC. Furthermore, in phase 2, a comparative analysis was conducted to develop the PbD framework, and hypotheses were articulated. Also, a survey instrument was developed and applied, where 386 responses were utilized to test the hypotheses. In the data analyses, the quantitative analysis was implemented based on SEM-PLS, and the output is the PbD framework. In phase 3, a quantitative methodology is applied to validate the PbD framework using SEM-PLS model fit, and the output validates the PbD framework. Overall, this chapter discussed the research process and Literature Analysis. In addition, the chapter explains the development of survey instruments, data collection and analyses, instrument, validity

and reliability, data collection and data analyses, SmartPLS, measurement model and structural model, and finally, a chapter summary. The next chapter presents the result and discussion.

CHAPTER 5: RESULTS AND DISCUSSION

This current chapter shows the result and discussion, including data collection, the result of the measurement model, and result of the structural model, and finally, a summary of the chapter.

5.1 Results of the Demographic Analysis

As shown in Table 5.1, a total of 386 respondents were received, including 306 Male (79.27%) and 80 Females (20.73%). The result shows that a group of 195 participants aged 30 years to 39 years old represents the highest percentage age group of the respondents with a percentage of 50.52%, followed by 114 participants aged 20 years to 29 years old with a percentage of 20.73%.

In addition, as presented in Table 5.1, a total of 306 of the 386 participants are male in the gender group and 234 of 386 (60.62%) were married.

Moreover, as shown in Table 5.1, the education level of the respondents shows a percentage of 49.74% (192) with a Bachelor's degree, followed by a percentage of 39.38% (152) with a Master's degree, respectively.

As presented in the questionnaire, in the cloud storage question, the respondents were asked about their most-used cloud storage to save their personal data gathered from their mobile devices. However, each respondent must make only one choice for the answer. The choices include Google Drive, Dropbox, One Drive, iCloud, and others, as clarified as follows:

a) Google Drive: It is developed by Google to store and synchronize services, which allows the users who want to store files in google drive servers and use other Google drive services (Quick & Choo, 2014).

b) ICloud: It has been developed by Apple Inc. as a cloud storage service to help users store their data such as photos, music, and documents on remote servers (Oh et al., 2012).

c) One drive: It was previously known as SkyDrive. It was developed by Microsoft to store files and synchronization services as part of its Office web product (Quick & Choo, 2013).

d) Dropbox: It is a file holding service run by an American company Dropbox, Inc. Dropbox offers the user's cloud storage (Quick & Choo, 2013).

Based on the utilization of cloud storage, Table 5.1 shows that most of Google Drive have a percentage of 45.85% (177), followed by iCloud and Dropbox with 21.24% (82) and 16.32% (63), respectively.

Table 5.1: A statistics of demographic characteristics of participants

Demographic	Category	Number of participate.	Percentage
Age	19 or younger	3	0.78%
	20 to 29	114	29.53%
	30 to 39	195	50.52%
	40 or older.	74	19.17%
Gender	Female	80	20.73%
	Male	306	79.27%
Marital Status	Single	135	34.97%
	Married	234	60.62%
	Divorced	17	4.40%
Education level	Ph.D. / Doctorate	26	6.74%
	Master's degree	152	39.38%
	Bachelor's degree	192	49.74%
	High school diploma	14	3.63%
	Elementary / Primary education	2	0.52%
Cloud storage	Google Drive	177	45.85%

	iCloud	82	21.24%
	Dropbox	63	16.32%
	One Drive (formerly Sky Drive)	31	8.03%
	Others	33	8.55%

As shown in Table 5.1, almost 80% of the respondents in this study were male. To confirm the sample, previous researchers have investigated whether gender affects privacy concerns (Dommeyer & Gross, 2003). As a result, several of these studies have not revealed any gender effect, and no statistically significant differences were found between females and males (Dommeyer & Gross, 2003). Therefore, having 80% of the respondents being male will not affect the results (Dommeyer & Gross, 2003).

For types of questions and responses from respondents, the questions are 5-point Likert scale, and more importantly, all the questions are mandatory; the unfinished survey is automatically not allowed to continue. Accordingly, all the samples of the 386 responses were completed by answering all the survey questions.

In this research, PLS in SmartPLS 3.2.8 (Ringle et al., 2005) was utilized to analyze the collected data. Specifically, PLS is suitable for describing complex relationships as it avoids undesirable issue solutions and does not identify variables (Fornell & Larcker, 1981).

5.2 Results of the Measurement Model

As mentioned in the previous research, the measurement model comprises the relationship between latent variables and their (item) indicators (Sarstedt et al., 2017; Williams et al., 2014). In this research, the standard convergent validity, reliability, and discriminant validity (Williams et al., 2014) were utilized to reflectively measure constructs.

5.2.1 Results of Convergent Validity and Reliability

As illustrated in Table 5.2, all scales demonstrate adequate values with a Cronbach's alpha (CA) score greater than 0.70, composite reliability (CR) scores higher than 0.70, and average variance extracted (AVE) score higher than 0.50 (Ab Hamid et al., 2017). According to the findings in Table 5.2, researchers have found:

a) Results of average variance extracted (AVE): Based on the demonstration of several researchers, the AVE should be at least 0.5 to be at a satisfactory level (Shmueli et al., 2019; Hair Jr et al., 2017; Chin, 2010; Fornell & Larcker, 1981; Nunnally, 1978).

b) Results of Cronbach's alpha (CA): Litwin (1995) recommended the value of Cronbach's alpha should be greater than 0.7, while Churchill (1979) and Chin (1998) suggest that it is acceptable to take the internal consistency of the CA value with 0.6 (Sarstedt et al., 2017; Chin, 1998b; Litwin, 1995; Churchill Jr, 1979). According to Hair et al. (Hair Jr et al., 2017; Hair et al., 2010), Cronbach's alpha with a starting range of 0.713 to 0.917 is acceptable (Sarstedt et al., 2017; Hair et al., 2010).

c) Results of composite reliability (CR): According to the presentation of Chin (2010), Fornell and Larcker (1981), and Nunnally (1978), if the CR score is above 0.70 then it is satisfactory (Shmueli et al., 2019; Chin, 2010; Fornell & Larcker, 1981; Nunnally, 1978).

d) Results of variance inflation factor (VIF): Based on Petter et al. (Petter et al., 2007), Williams et al. (2014), Hair et al. (2016), Scott (2020), and Sarstedt et al. (2017), the VIF value in the range of 3.3 or 5.0 thresholds is recommended. In this research, variance inflation factor values varied from 1.293 to 2.741. Consequently, the outcome in Table 5.2 offered evidence that multicollinearity is not a threat to the validity of the measurements (Scott, 2020; Williams et al., 2014). In addition, Table 5.2 shows that all reflecting indicator loadings overtook the acceptable value of 0.60, as suggested in (Yacob et al., 2017; Bagozzi & Yi, 1988). Also, the loading item has

a minimum value of 0.50 and is acceptable (Kamis, 2021; Chua, 2018; Hair et al., 2006).

Table 5.2: Convergent validity

Constructs	Items	Loading	VIF	Cronbach's Alpha	CR	AVE
Perceived Severity	P. SEV1	0.805	1.696	0.752	0.835	0.504
	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	0.762	0.849	0.586
	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	0.871	0.903	0.608
	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	0.764	0.847	0.582
	P. BAR2	0.817	1.516			
	P. BAR3	0.792	1.696			
	P. BAR4	0.716	1.584			
Cues to action of Privacy by design	CAPD1	0.699	1.561	0.864	0.898	0.597
	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	PDBPMCC1	0.728	1.610	0.876	0.910	0.671
	PDBPMCC2	0.819	2.048			

behavior in MCC	PDBPMCC3	0.868	2.557			
	PDBPMCC4	0.830	2.626			
	PDBPMCC5	0.844	2.741			

Note: Cronbach's alpha (CA) score higher than 0.70, composite reliability (CR) scores greater than 0.70, and average variance extracted (AVE) score greater than 0.50.

5.2.2 Results of Discriminant Validity

As presented in Table 5.3, the cross-loadings achieved sufficient values (with yellow highlights). According to Hair et al. (2011), every measurement item must load greater on its key construct than on any other fundamental construct (Kamis, 2021; Hair et al., 2011). In this research, cross-loading measures present sufficient discriminant validity and are satisfied based on Gefen et al. (Gefen & Straub, 2005; Gefen et al., 2000). As Gefen et al. reported, "the measures should load more on their hypothesized construct than on others to evaluate the convergent and discriminant validity of the reflective measures" (Gefen et al., 2000). Conceding to the acknowledgment of Gefen et al., the hypothesized construct of the item loadings should be at least 0.10 higher compared to item cross-loading on that construct (Kamis, 2021; Gefen & Straub, 2005).

Table 5.3: Cross loading

	P.BEN	P.BAR	CAPD	P.SUS	P.SEV	PDPBMCC
P.BEN1	**0.716**	0.350	0.558	0.209	0.227	0.454
P.BEN2	**0.742**	0.292	0.525	0.181	0.192	0.431
P.BEN3	**0.822**	0.291	0.547	0.178	0.173	0.536
P.BEN4	**0.834**	0.259	0.539	0.122	0.120	0.552
P.BEN5	**0.740**	0.185	0.497	0.070	0.106	0.524
P.BEN6	**0.817**	0.301	0.511	0.212	0.272	0.594
P.BAR1	0.255	**0.721**	0.357	0.390	0.359	0.255
P.BAR2	0.342	**0.817**	0.458	0.428	0.439	0.304
P.BAR3	0.258	**0.792**	0.391	0.567	0.562	0.249
P.BAR4	0.198	**0.716**	0.324	0.561	0.500	0.167
CAPD1	0.414	0.369	**0.699**	0.242	0.223	0.440
CAPD2	0.570	0.348	**0.787**	0.203	0.183	0.598
CAPD3	0.602	0.420	**0.804**	0.279	0.295	0.626
CAPD4	0.444	0.378	**0.706**	0.267	0.311	0.524
CAPD5	0.558	0.378	**0.826**	0.225	0.239	0.596
CAPD6	0.519	0.464	**0.804**	0.299	0.288	0.598
P.SUS1	0.227	0.499	0.349	**0.787**	0.530	0.248
P.SUS2	0.127	0.493	0.220	**0.844**	0.538	0.167

P.SUS3	0.128	0.436	0.274	**0.711**	0.422	0.255
P.SUS4	0.146	0.469	0.157	**0.711**	0.483	0.104
P.SEV1	0.200	0.452	0.257	0.511	**0.805**	0.220
P.SEV2	0.100	0.443	0.199	0.494	**0.753**	0.149
P.SEV3	0.129	0.348	0.167	0.375	**0.653**	0.138
P.SEV4	0.264	0.532	0.351	0.486	**0.666**	0.295
P.SEV5	0.128	0.337	0.203	0.418	**0.661**	0.180
PDPBMCC1	0.456	0.334	0.575	0.293	0.326	**0.728**
PDPBMCC2	0.526	0.297	0.637	0.188	0.251	**0.819**
PDPBMCC3	0.545	0.268	0.644	0.211	0.203	**0.868**
PDPBMCC4	0.558	0.226	0.563	0.168	0.192	**0.830**
PDPBMCC5	0.637	0.225	0.584	0.174	0.167	**0.844**
Note: P.BAR = Perceived Barriers; P.BEN = Perceived Benefits; CAPD = Cue to Action of privacy by design; P. SUS = Perceived Susceptibility; P.SEV = Perceived Severity; PDPBMCC = Privacy and personal data protection behavior in MCC.						

As illustrated in Table 5.4, the discriminant validity (Fornell-Larcker criterion) of a construct is evaluated by comparing the correlations among constructs with the square root of the AVE for a construct (Fornell & Larcker, 1981). Fornell-Larcker criteria provided sufficient values (highlighted in yellow), where the value of the key construct is greater than the value of the other constructs (Kamis, 2021; Al-Maroof & Al-Emran, 2018; Fornell & Larcker, 1981). As presented in Table 5.4, the items in the matrix diagonals representing the AVEs' square root are always higher than the off-diagonal items in the corresponding column and row (Kamis, 2021), obtaining demonstrating discriminant validity.

The discriminant validity values had been fulfilled based on Fornell-Larcker (Fornell-Larcker Criterion) recommendation, as presented in Table 5.4 (Al-Maroof & Al-Emran, 2018; Fornell & Larcker, 1981).

Table 5.4: A 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**

The Heterotrait-Monotrait Ratio (HTMT) has suggested a threshold value of 0.90, which implies that the value above 0.90 lack discriminant validity (Aldholay et al., 2018; Henseler et al., 2015). Moreover, the HTMT confidence interval should not have a value of one (Tehseen et al., 2017). The approach is utilized by Smart PLS 3 to fulfill the HTMT discriminant validity. In this study, as illustrated in Table 5.5, based on HTMT's PLS performance, the result shows that the HTMT criterion in this study was achieved.

Table 5.5: Heterotrait-Monotrait Ratio (HTMT)

	CAPD	**P.BAR**	**P.BEN**	**P.SEV**	**P.SUS**	**PDPBMCC**
CAPD						
P.BAR	0.615					
P.BEN	0.779	0.426				
P.SEV	0.411	0.799	0.288			
P.SUS	0.403	0.834	0.256	0.850		
PDPBMCC	0.839	0.390	0.756	0.343	0.311	

5.2.3 Second-order

In this research, the perceived threat measure was modeled as a second-order where the second-order construct is considered as the latent variable, and the first-degree construct is worked as an indicator (Chua, 2018; Wetzels et al., 2009). The perceived threat comprises perceived susceptibility and perceived severity as two fundamental aspects (Glanz et al., 2008). As presented in Figure 5.1, the paths of the underlying perceived threat dimensions are significant (SUS: b=0.529, p<0.001; SEV: b=0.571, p<0.001). Also, as shown in Figure 5.1, the path weights of all individual indicators on the second-order construct are significant at p<0.001.

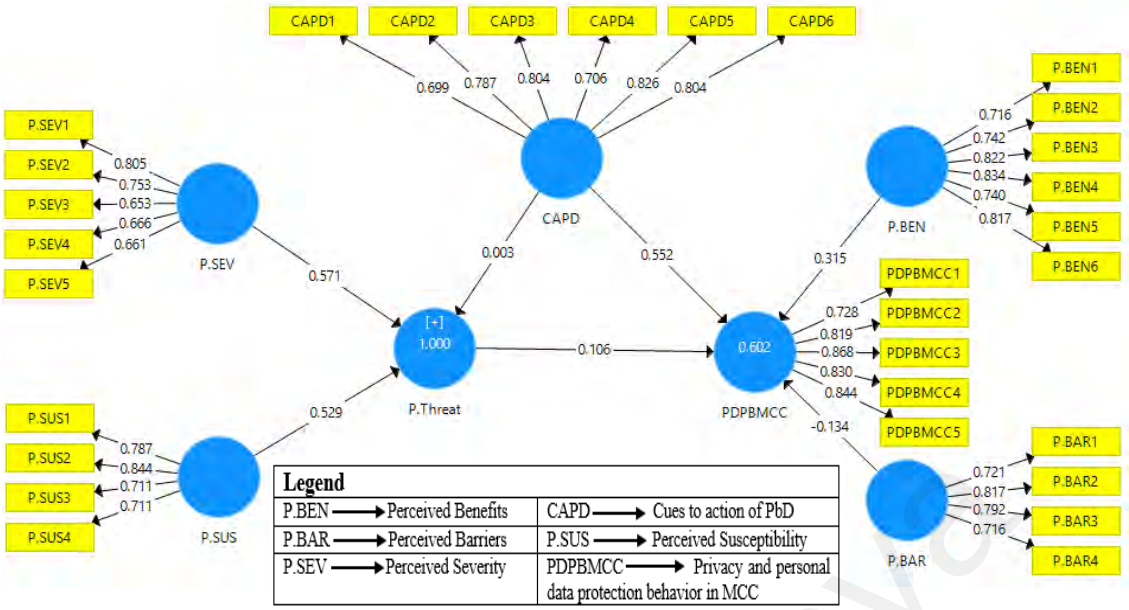


Figure 5.1: Result of SmartPLS

The proposed framework, as shown in Figure 3.6, is translated by the SmartPLS software in the analysis. In other words, Figure 5.1 demonstrates the proposed research framework in the SmartPLS worksheet after the assessment had been conducted. The quantitative analysis was done using SEM-PLS for the data analysis. Figure 5.1 shows the Latent endogenous variable PDPBMCC, having an R^2 of 0.602. In addition, Figure 5.1 presents the positive relation of P.BEN to PDPBMCC with a value of 0.315, the negative relation of P.BAR to PDPBMCC with a value of -0.134, positive relation of CAPD to PDPBMCC with a value of 0.552, and positive relation of P.Threat to PDPBMCC with a value of 0.106. Moreover, there is a positive relation between CAPD and P.Threat with a value of 0.003. Furthermore, P.Threat was demonstrated as a second-order where the second-order construct is considered as the latent variable, and the first-degree construct is worked as an indicator that included P.SEV and P.SUS, which in turn indicated that all items of P.SEV and P.SUS are included in P.Threat.

5.3 Results of the Structural Model

After assessing the measurement model in this research, the structural model was evaluated. Specifically, the structural model comprises the model's hypothesized relationship between endogenous and exogenous variables. The outcome of the structural

model, include the Hypotheses testing (Path coefficient), Effect size (f^2), Predictive relevance Q^2, Coefficient of determination R^2, and Goodness of Fit of the Model- GoF.

5.3.1 Coefficient of Determination (R^2)

The computed model's explanatory power may be assessed by tracking the R^2 of the endogenous constructs. Chin recommends that R^2 values more than 0.67 should be regarded as strong, values between 0.33 and 0.67 should be considered moderate, values between 0.19 and 0.33 considered weak, and R^2 values less than 0.19 should be avoided (Chin, 1998b). Also, one study suggested an R^2 value of 0.10 as the lowest acceptable limit (Kassem et al., 2020). The R^2 value gotten from the analysis was 0.602, suggesting that all exogenous variables in the model can explain 60.2 % of the variation (Kassem et al., 2020; Falk & Miller, 1992).

The R-squared (R^2) value of the endogenous variable is used in PLS analysis to assess the predictive capacity of a certain construct or model and to calculate the standard path coefficient of each connected endogenous and exogenous variable (Janadari et al., 2016). Hair et al. (2016) recommended that the range of R^2 is from 0 to 1. The authors also suggested that the R^2 value of 0.25 is considered weak, a value of 0.50 deemed to be moderate, and a value of 0.75 considered substantial in endogenous latent variables, as a rule of thumb. In this research, as displayed in Table 5.6, the R^2 value of the endogenous construct is considered moderate, which is recommended (Chin, 1998b).

Table 5.6: Coefficient of determination (R^2)

R-square of the Endogenous Latent Variables		
Constructs Relation	**R Square**	**Result**
PDPBMCC	0.602	Moderate

5.3.2 Effect Size (f^2)

Effect size (f^2) is a statistical term that measures the correlation strength among two variables on a numerical scale (Cohen, 1988). Effect size evaluates the effect of particular exogenous constructs on the endogenous construct. Furthermore, f^2 allows the

interpretation of an endogenous construct to be measured in increments and thus provides proof of the predictive capabilities of the model (Henseler et al., 2009). As per Cohen (1988), values for evaluating effect size (f^2) for the exogenous constructs can also be defined as large, medium, and small in predicting the endogenous constructs (Cohen, 1988). Also, the value of 0.01 is considered very small (Hosseini et al., 2018; Abd Razak et al., 2016; Sawilowsky, 2009), the value of 0.02 is considered small (Hosseini et al., 2018; Cohen, 1988), the value of 0.15 is considered medium (Cohen, 1988), the value 0.35 is considered large (Henseler et al., 2016; Cohen, 1988), the value of 1.20 is very large (Phinyomark et al., 2018; Sawilowsky, 2009), and the value of 2.0 is huge (Phinyomark et al., 2018; Sawilowsky, 2009). Table 5.7 illustrates the obtained result of the effect size of this study.

Table 5.7: Effect size (f^2)

Constructs	f^2	Inference
CAPD-> P.Threat	0.063	small
CAPD -> PDPBMCC	0.352	large
P.BAR -> PDPBMCC	0.021	small
P.BEN -> PDPBMCC	0.135	medium
P.SEV -> P.Threat	1.327, 7	large
P.SUS -> P.Threat	1.143, 8	large
P. Threat -> PDPBMCC	0.015	very small

5.3.3 Predictive Relevance Q^2

Predictive relevance (Q^2) is the capacity of the model for measuring or predicting the endogenous variables (Janadari et al., 2016). As per Chin et al. (2010), The Q^2 may be utilized as a predictive relevance criterion (Chin, 2010). The Q^2 assesses predictive validity via the blindfolding process in which data is removed for a specific indicator block and then predicts the deleted portion based on the calculated parameters (Sarstedt et al., 2017).

Therefore, Q^2 demonstrates how effective the empirically gathered data may be rebuilt by utilizing PLS-SEM parameters and the model (Tehseen et al., 2017; Hair Jr et al., 2016; Akter et al., 2011). As proposed by Chin (2010), Q^2 was achieved via a coefficient of determination procedure (Chin, 2010). Furthermore, Hair et al. (2016) suggested that the predictive relevance of the model occurs when Q^2 is larger than 0, while Q^2 lacks the predictive relevance of the model when Q^2 is less than 0 (Kassem et al., 2020; Hair Jr et al., 2016). In this study, as presented in Table 5.8, the Q^2 value is above 0 for both P. Threat and PDPBMCC.

Table 5.8: Predictive relevance Q^2

	SSO	SSE	Q^2 (=1-SSE/SSO)
CAPD	2,316.000	2,316.000	
P.BAR	1,544.000	1,544.000	
P.BEN	2,316.000	2,316.000	
P.SEV	1,930.000	1,930.000	
P.SUS	1,544.000	1,544.000	
P.Threat	3,474.000	2,033.930	**0.415**
PDPBMCC	1,930.000	1,204.320	**0.376**
Note: The Q^2 = SSO / 1 SSE, which is the model's predictive correlation with the endogenous variables, where SSE is the sum of the squares prediction errors, and SSO is the sum of the squares observations (Sha et al., 2017; Wong, 2016).			

5.3.4 The Goodness of Fit of the Model-GoF

Tenenhaus et al. (2005) introduced the Goodness of Fit index (GoF), which considers the performance of both the structural and measurement models (Kassem et al., 2020; Henseler & Sarstedt, 2013). The overall goodness of fit of the model should be the starting point for model evaluation. Thus, if the model does not use the data correctly then the data includes more information than the model provides (Henseler et al., 2016). The estimates obtained may be unmeaning, and the outcomes drawn from them may become questionable (Henseler et al., 2016). The GoF index is essential for assessing the global validity of the complex PLS-based model (Tenenhaus et al., 2005). Moreover, the GoF is

known as the geometric mean of average R^2 and the average commonality for all endogenous constructs (Onumo et al., 2021). Generally, several studies have evidenced the importance of these techniques (Onumo et al., 2021; Kassem et al., 2020; Chao, 2019; Akter et al., 2011). The researchers used the Goodness of Fit measure to give evidence in support of the research model (Onumo et al., 2021; Akter et al., 2011).

The criteria of Goodness of Fit to define GoF values for R^2 can be calculated using the following equation (Kassem et al., 2020):

$$GoF = \sqrt{(\overline{R^2} \times \overline{AVE})} \quad (1)$$

In the values of GoF, if the value is more than 0.36 (large), between 0.25 to 0.36 (medium), between 0.1 to 0.25 (small), and if it is less than 0.1 (no fit) cannot be considered as a global valid PLS model and it has been given by Wetzels et al. (2009) (Adjei et al., 2021; Azizah & Puspito, 2021; Akter et al., 2011; Wetzels et al., 2009). In this study, as illustrated in Table 5.9, the statistical results of the current model achieved a GoF value of 0.596, indicating large.

Table 5.9: The Goodness of Fit of the Model-GoF

	R^2	Constructs	AVE		
		P.BEN	0.608		
		P.BAR	0.582		
		CAPD	0.597		
		P.SUS	0.586		
		P.SEV	0.504		
		PDPBMCC	0.671		
Average	**0.602**		**0.59133**		
Multiplication R^2 *AVE				**0.355983**	
Square root					**0.596643**

Legend: R^2= Coefficient of determination. AVE= Average Variance Extracted

5.3.5 Hypotheses Testing (Path Coefficient)

As shown in Table 5.10 and Figure 5.1, the hypothesis test outcome of PPDP behavior in mobile cloud computing was analyzed by utilizing the path analysis model (Xhafaj et al., 2021; Puspita et al., 2017). The outcomes of hypotheses testing and analysis are discussed as follows:

H1: Perceived benefits are positively related to privacy and personal data protection behavior in mobile cloud computing.

As presented in Table 5.10 and Figure 5.1, the outcome of this thesis is highly supported that the perceived benefits are positively related to PPDP behavior in mobile cloud computing (SE = 0.56, $\beta = 0.315$, $p = 0.000$). Compared to previous studies in the domain, the current finding has resulted in the same finding of Koloseni et al. (2019), Williams et al. (2014), Humaidi & Balakrishnan (2012), Claar & Johnson (2010), and Ng et al. (2009).

The result presented in Chet L Claar & Johnson, 2010 supported the hypothesis that the perceived benefits of practicing computer security are positively related to computer security usage. Furthermore, the result shown by Ng et al., 2009 supported the hypothesis that the perceived benefits of practicing computer security are positively related to computer security behavior. The outcome demonstrated by Humaidi & Balakrishnan, 2012 supported the hypothesis that the perceived benefits influence users' behavior toward information security. Furthermore, the result illustrated in Williams et al., 2014 supported the hypothesis that an individual employee's perceived benefits of preventive behaviors are positively associated with intentions to perform preventive security behaviors. Additionally, the result explained by Koloseni et al., 2019 supported the hypothesis that the perceived benefits have a positive influence on the intention of employees to practice information security behavior (Koloseni et al., 2019; Williams et al., 2014; Humaidi & Balakrishnan, 2012; Claar & Johnson, 2010; Ng et al., 2009).

H2: Perceived barriers are negatively related to privacy and personal data protection behavior in mobile cloud computing.

As presented in Figure 5.1 and Table 5.10, the outcome is highly supported where perceived barriers are negatively related to PPDP behavior in mobile cloud computing (SE = 0.52, β = -0.134, p = 0.005). Connected to the results of previous studies, the hypothesis related to the perceived barriers are negatively related to the current hypothesis resulting in the same outcome as presented by Koloseni et al. (2019), Humaidi & Balakrishnan (2015), Williams et al. (2014), Claar and Johnson (2010), and Ng et al. (2009).

Table 5.10: Hypothesis testing

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		Supported*
H4	CAPD → PDPBMCC	0.552	0.056	9.884	0.000	0.602	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*

The significance at P**=<0.01, P*<0.05.

The result shown by Ng et al. (2009) supported the hypothesis that the perceived barriers of practicing computer security are negatively related to computer security behavior. Claar and Johnson (2010) supported the hypothesis that the perceived barriers of practicing computer security are negatively related to computer security usage. Humaidi & Balakrishnan, 2015 supported the hypothesis that the perceived barriers influence users' implementing information security policies (ISPs) compliance behavior. Williams et al., 2014 supported the hypothesis that an individual employee's perceived barriers to preventive security behaviors are negatively associated with their intentions to perform preventive security behaviors. Koloseni et al. (2019) supported the hypothesis

that the perceived barriers have a negative influence on the intention of employees to practice information security behavior (Koloseni et al., 2019; Humaidi & Balakrishnan, 2015; Williams et al., 2014; Claar & Johnson, 2010; Ng et al., 2009).

H3: Cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to the perceived threat.

As presented in Table 5.10 and Figure 5.1, the outcome is supported that cues to action of PbD considering visibility location transparency, laws, and regulations are positively related to the perceived threat (SE = 0.001, β = 0.003, p = 0.015), which is committed to the declaration of Edwards (Edwards, 2015), where the cues to action are positively related to a person's perception of an event being a security threat (Edwards, 2015).

H4: Cues to action of privacy by design, considering visibility location transparency, laws, and regulations are positively related to privacy and personal data protection behavior in mobile cloud computing.

As illustrated in Figure 5.1 and Table 5.10, the result is highly supported that cues to action of privacy by design, considering visibility location transparency, laws, and regulations are positively related to PPDP behavior in mobile cloud computing (SE = 0.056, β = 0.552, p = 0.000), and it confirmed the findings of other studies in the domain for similar hypothesis, including studies by Koloseni et al. (2019), Williams et al. (2014), Humaidi & Balakrishnan (2012), Claar & Johnson (2010), and Ng et al. (2009).

The result of Claar and Johnson (2010) supported the hypothesis that the cues to action are positively related to computer security usage. Moreover, the result of Ng et al. (2009) supported the hypothesis that the cues to action are positively related to computer security behavior. The result of Koloseni et al. (2019) supported the hypothesis that the cues to action have a positive influence on the intention of employees to practice information security behavior. Furthermore, the result of Williams et al., 2014 supported the hypothesis that the cue to action is positively related to an individual employee's intention

to perform preventive information security behaviors. Additionally, the result of Humaidi & Balakrishnan, 2012 supported the hypothesis that the cues to action influence users' behavior toward information security (Koloseni et al., 2019; Williams et al., 2014; Humaidi & Balakrishnan, 2012; Claar & Johnson, 2010; Ng et al., 2009).

H5: Perceived threat is positively related to privacy and personal data protection behavior in mobile cloud computing.

As demonstrated in Table 5.10 and Figure 5.1, the outcome is supported that the perceived threat is positively related to PPDP behavior in mobile cloud computing (SE = 0.043, $\beta = 0.106$, $p = 0.007$). Also, the most interesting finding was that this investigation draws the same proceeding as a previous study by Edwards (Edwards, 2015) that perceived threat is positively related to a person's security behavior (Edwards, 2015).

H6: Perceived severity is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

As presented in Figure 5.1 and Table 5.10, the outcome of this study supported the hypothesis (SE = 0.025, $\beta = 0.60$, $p = 0.007$) that the perceived severity is positively related to PPDP behavior in mobile cloud computing through perceived threat. Compared to other studies in the domain, this finding is considered to be the same as the previous work presented by Koloseni et al. (2019), Humaidi & Balakrishnan (2015), Williams et al. (2014), and Ng et al. (2009).

In brief, Ng et al. (2009) supported the hypothesis that the perceived severity of security incidents is positively related to computer security behavior (Ng et al., 2009). Humaidi & Balakrishnan, 2012 supported the hypothesis that the perceived severity of security incidents influences users' behavior toward information security (Humaidi & Balakrishnan, 2012). Also, Humaidi & Balakrishnan (2015) supported the hypothesis that the user's awareness of the perceived severity influences the user's implementing information security policies (ISPs) compliance behavior (Humaidi & Balakrishnan,

2015). Koloseni et al. (2019) supported the hypothesis that perceived severity has a positive influence on the intention of employees to practice information security behavior (Koloseni et al., 2019). Williams et al., 2014 supported the hypothesis that the individual employee's overall perceived severity of outcomes related to particular security violations are positively associated with the individual's intentions to perform preventive security behaviors (Williams et al., 2014).

H7: Perceived susceptibility is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

As demonstrated in Figure 5.1 and Table 5.10, the outcome of this study supported the hypothesis (SE = 0.023, $\beta = 0.56$, $p = 0.007$) that the perceived susceptibility is positively related to PPDP behavior in mobile cloud computing through perceived threat. Compared to other previous studies in the domain, the result is considered to be the same finding as the previous work done by Koloseni et al. (2019), Humaidi & Balakrishnan (2015), Williams et al. (2014), and Ng et al. (2009).

In summary, Ng et al. (2009) supported the hypothesis that the perceived susceptibility to security incidents is positively related to computer security behavior (Ng et al., 2009). Humaidi & Balakrishnan, 2012 supported the hypothesis that perceived susceptibility influences users' behavior toward information security (Humaidi & Balakrishnan, 2012). Also, Humaidi & Balakrishnan, 2015 supported the hypothesis that the user's awareness of perceived susceptibility influences the user's ISPs compliance behavior (Humaidi & Balakrishnan, 2015). Koloseni et al. (2019) supported the hypothesis that perceived susceptibility has a positive influence on the intention of employees to practice information security behavior (Koloseni et al., 2019). Williams et al., 2014 supported the hypothesis that an individual employee's perceived susceptibility to particular security violations is positively associated with intentions to perform preventive security behaviors (Williams et al., 2014). Figure 5.2 shows the validated PbD framework.

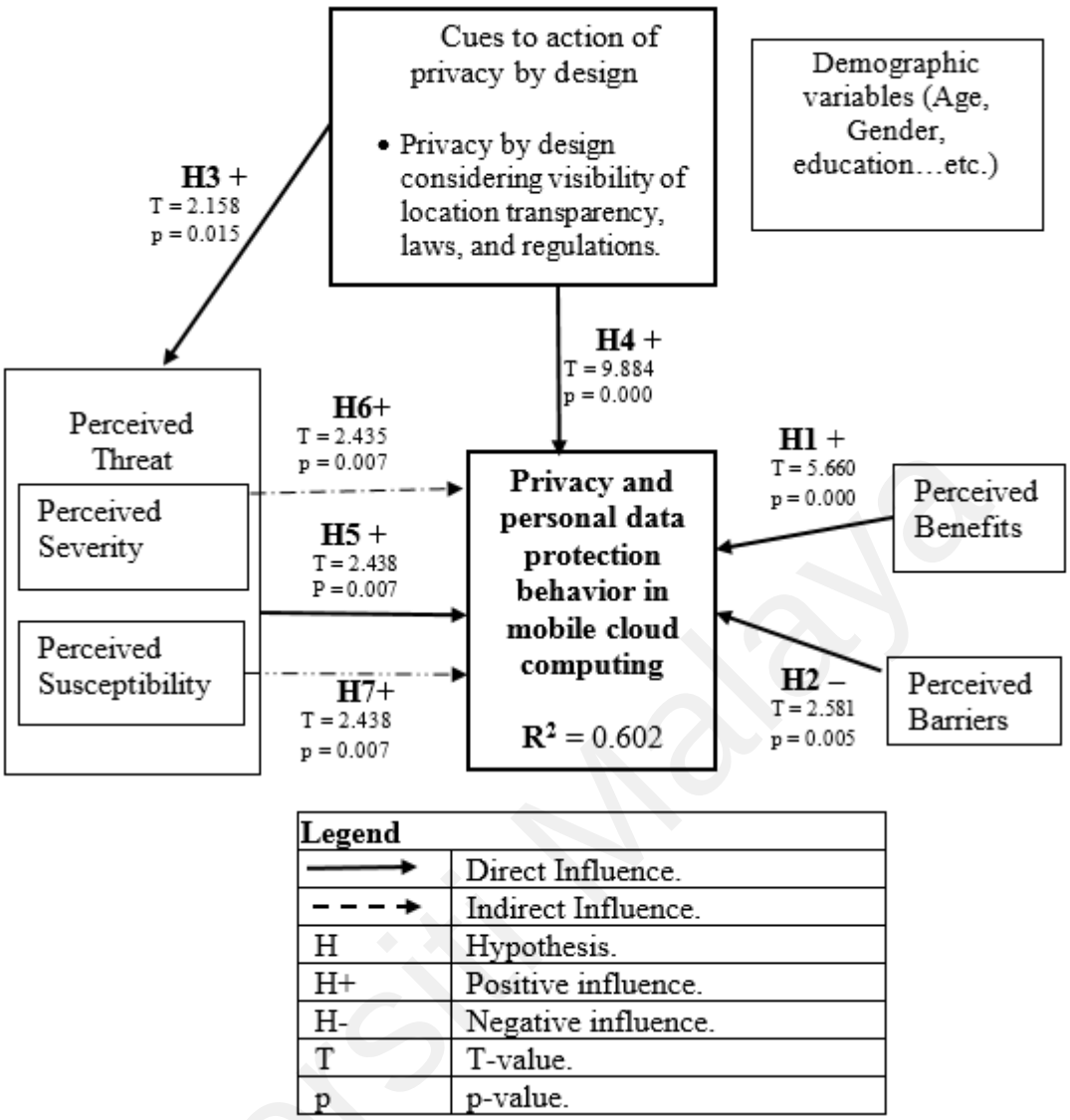


Figure 5.2: Validated PbD Framework

5.4 Summary

This chapter illustrates the result and discussion, including data collection, results of the measurement model, and results of the structural model. The next chapter will present the research conclusion and future work.

CHAPTER 6: CONCLUSION AND FUTURE WORK

This current chapter shows a summary of the principal findings, limitations, contributions, and conclusion and future research of this thesis.

6.1 Summary of Principal Findings

In this research, three phases were implemented to achieve the objectives. The first phase is the Literature Analysis through which RO1 and RO2 were achieved. In phase 2, the PbD framework was developed, a comparative analysis was conducted, and hypotheses were articulated. Also, a survey instrument was developed and implemented in which 386 responses were utilized to test the hypotheses. In the data analyses, the quantitative analysis was carried out using the SEM-PLS, and the output is the PbD framework. In phase 3, the PbD framework was validated, a quantitative methodology is applied using SEM-PLS model fit, and the output validates the PbD framework. In summary, the principal findings of this research in achieving the research objectives are highlighted as follows:

i. RO 1: To identify existing data privacy threats and existing solutions proposed to preserve privacy and personal data protection in MCC.

To achieve RO 1, a Systematic-mapping-study was conducted, where 1711 papers published from the year 2009 to the year 2019 were collected, followed by a process of filtering, and as a result, 74 primary studies were selected and investigated where the current data privacy attacks and threats in mobile cloud computing (MCC) were identified, and the current privacy solutions proposed to preserve personal data protection in the MCC were observed.

In the conducted SMS, the current data privacy attacks and threats in the MCC were identified. The outcomes show that the most common attacks and threats presented in the 74 selected primary studies are unauthorized attacks and threats, which is illustrated in

18% of the selected primary studies, followed by leakage of user privacy, data privacy, data misuse, and untrusted service provider with 15%, 13%, and 11% of the chosen primary studies, respectively. Moreover, disclosing the information or the data, and man-in-the-middle attacks are in 6% and 5% of the selected primary studies. Furthermore, the result of SMS shows that there is a lack of research on internal attacks, data breach threats, improper security practices and policies in some locations, inference attacks on user privacy, eavesdropping attacks, and internal multi-layer attacks.

In the conducted SMS, the existing data privacy solutions projected to preserve personal data protection in mobile cloud computing were identified. The result displays that the studies concentrated on encryption with 50%, authentication with 28%, and access control with 19%. Moreover, this study noted that researchers have begun to suggest trust as a solution in the MCC field, where there are only two primary studies that offer trust as a solution. Furthermore, the result of the SMS has not shown any proposed solution that utilizes the PbD solution to preserve PPDP in the MCC.

ii. RO 2: To investigate the determinants that influence the preservation of privacy and personal data protection in the MCC.

To achieve RO 2, a systematic literature review (SLR) was conducted. In the SLR, a total of 378 primary studies were identified; however, 19 primary studies were selected after a filtering process, investigated and used to determine the determinants that influence the preservation of PPDP in the MCC.

The conducted SLR has identified determinants that are used for preserving privacy and security in information systems. In the SLR, a total of 37 determinants in 19 studies were identified and investigated to determine the determinants that influence the preservation of PPDP in the MCC.

iii. RO 3: To develop privacy by design framework to preserve privacy and personal data protection in the MCC.

iv. RO 4: To validate the privacy by design framework in preserving privacy and personal data protection in the MCC.

To achieve RO 3 and RO 4, a framework was projected to preserve PPDP in the MCC utilizing PbD. This study is contributed to enterprise architecture and information systems security in mobile cloud computing by preserving PPDP in the MCC. The proposed framework uses PbD visibility and transparency, considering location transparency, laws, and regulations.

A survey has been conducted to test the formulated hypotheses, where a questionnaire has been circulated and a pilot study conducted with 100 responses, and a total of 386 responses were received for the analyses. In the pilot study and the analyses, SmartPLS is utilized to analyze the collected data. Moreover, one of the most well-known software implementations for Partial Least Squares Structural Equation Modeling is SmartPLS (PLS-SEM). In summary, in this research, the results of the formulated hypotheses are presented as keen below:

- **H1:** Perceived benefits are positively related to privacy and personal data protection behavior in mobile cloud computing.

The outcome of this thesis is highly supported that the perceived benefits are positively related to PPDP behavior in mobile cloud computing (SE = 0.56, β = 0.315, p = 0.000). Compared to previous studies in the domain, the current finding has resulted in similar findings as by Al-diabat (2019), Schymik & Du (2017), Sekyere (2015), Williams et al. (2014), and Ng et al. (2009).

- **H2:** Perceived barriers are negatively related to privacy and personal data protection behavior in mobile cloud computing.

The outcome of this study is highly supported that the perceived barriers are negatively related to PPDP behavior in mobile cloud computing (SE = 0.52, β = -0.134, p = 0.005). Connected to the outcomes of previous studies, the hypothesis related to the perceived

barriers are negatively associated with the current hypothesis resulting in the same outcome as presented by Koloseni et al. (2019), Williams et al. (2014), Humaidi et al. (2012), Claar and Johnson (2010), and Ng et al. (2009).

- **H3:** Cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to the perceived threat.

The outcome of this study is supported that cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to the perceived threat (SE = 0.001, β = 0.003, p = 0.015) which is committed to the declaration of Edwards (Edwards, 2015), where the cues to action are positively related to a person's perception of an event being a security threat (Edwards, 2015).

- **H4:** Cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to privacy and personal data protection behavior in mobile cloud computing.

The outcome of this research is supported that cues to action of privacy by design considering visibility location transparency, laws, and regulations are positively related to PPDP behavior in mobile cloud computing (SE = 0.056, β = 0.552, p = 0.000), which confirmed the findings of other studies in the domain for similar hypothesis, including studies of Koloseni et al. (2019), Williams et al. (2014), Humaidi and Balakrishnan (2012), Claar and Johnson (2010), and Ng et al. (2009).

- **H5:** Perceived threat is positively related to privacy and personal data protection behavior in mobile cloud computing.

The outcome of this research is supported that the perceived threat is positively related to PPDP behavior in mobile cloud computing (SE = 0.043, β = 0.106, p = 0.007). The most intriguing finding was that this investigation follows the same path as previous research by Edwards (Edwards, 2015) that perceived threat is positively related to a person's security behavior (Edwards, 2015).

- **H6:** Perceived severity is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

The outcome of this research supported the hypothesis (SE = 0.025, β = 0.60, p = 0.007) that the perceived severity is positively related to PPDP behavior in MCC through perceived threat. Compared to other studies in the domain, this finding is considered to be the same finding as the previous work presented by Koloseni et al. (2019), Williams et al. (2014), Humaidi and Balakrishnan (2012), and Ng et al. (2009).

- **H7:** Perceived susceptibility is positively related to privacy and personal data protection behavior in mobile cloud computing through perceived threat.

As demonstrated in Figure 5.1 and Table 5.10, the outcome of this study supported the hypothesis (SE = 0.023, β = 0.56, p = 0.007) that the perceived susceptibility is positively related to PPDP behavior in mobile cloud computing through perceived threat. Compared to other previous studies in the domain, the result is considered to be the same as the finding of the previous studies conducted by Koloseni et al. (2019), Williams et al. (2014), Humaidi and Balakrishnan (2012), and Ng et al. (2009).

6.2 Limitations

In this study, some limitations need to be declared in this thesis. First of all, as shown in Table 5.1, the respondents reported their most-used cloud storages are Google Drive with 45.85%, iCloud with 21.24%, and Dropbox with 16.32%; in total, those three-cloud storage are amounting to use by 83.41 % of the total respondents, which in turn pointed out that three cloud storage demonstrated the experience of respondents in MCC, which is considered as a limitation of this study. To mitigate this limitation, the result shows additional cloud storage, which is One Drive with 8.03% and others with 8.55%, in a total of 16.58 %, which helped the researcher to mitigate this limitation.

Second of all, as shown in Figure 4.8, the questionnaire is distributed and shared via only two online platforms, including Facebook and LinkedIn, which limits the sharing of

the questionnaire among respondents. To ease this limitation, research reported that LinkedIn and Facebook offer users several features such as search interest groups or individual search and search groups, which help to find the respondents (Hosain & Liu, 2020; Hoadley et al., 2010), and it helped to mitigate this limitation.

Moreover, the limitation of this research focused on privacy in terms of personal data protection and the users who have used cloud platforms in mobile cloud computing such as iCloud and Google Drive.

Those limitations and shortcomings in the conduct of the survey are acknowledged by the researcher, and those mitigations presented above are demonstrated to ease those limitations in the results of this research.

6.3 Contributions

For practitioners and researchers, this research can help researchers and practitioners to determine the effects of applying privacy by design for PPDP in mobile cloud computing. Moreover, this research can support the utilization of privacy and personal data protection (PPDP) to preserve PPDP in the MCC. Also, this study can help to encourage practitioners to use PbD to preserve PPDP in mobile cloud computing.

For MCC users, this research can help to preserve privacy due to an increase in privacy issues, especially when increasing the number of mobile cloud computing users. Currently, mobile devices are almost in the hand of many MCC users in many places. Also, this study can assist and encourage users to utilize mobile cloud computing since mobile devices are useful for users whenever and wherever they want. In addition, this research can help the MCC users to know their storage locations and enable them to select the storage location based on their privacy concerns.

In summary, the contributions of this study are as follows. This research highlights the current privacy threats in mobile cloud computing. Moreover, this study demonstrates the existing solutions that are utilized to preserve PPDP in mobile cloud computing.

Furthermore, this investigation introduced a new framework that utilizes PbD to preserve PPDP in mobile cloud computing. This study is contributed to enterprise architecture and information systems security in mobile cloud computing by preserving PPDP in MCC. This research developed a PbD framework to preserve PPDP in mobile cloud computing. Also, this research evaluated the PbD framework to preserve PPDP in mobile cloud computing.

6.4 Conclusion and Future Research

Mobile cloud computing is an attractive research area that has emerged from the combination of cloud computing and mobile devices (Juárez & Cedillo, 2017). Currently, several studies have been published in response to the increased interest in privacy and personal data protection. Privacy and personal data protection (PPDP) are being recognized as key data issues in the MCC. This study used a PbD framework to preserve personal data protection in the MCC.

This research projected a framework to preserve PPDP in the MCC by utilizing PbD. The proposed framework uses PbD visibility and transparency, considering location transparency, laws, and regulations. A survey was conducted to test the formulated hypotheses, where a questionnaire was distributed, a pilot study was conducted with 100 responses, and a total of 386 responses were received for the analyses. In the pilot study and the analyses, SmartPLS was utilized to analyze the collected data. The SmartPLS is a very distinguished software solution for Partial Least Squares Structural Equation Modeling (PLS-SEM).

The outcomes of this research supported that the perceived threat, perceived benefits, and cues to action of PbD are positively and directly affected PPDP behavior in mobile cloud computing. Furthermore, the outcomes supported that the perceived barriers are negatively and directly affected PPDP behavior in mobile cloud computing.

In general, privacy concern affects not just individuals but also corporations. Additionally, while working with organizations, there is a question of security (Hayes et al., 2020). Therefore, for generalizing the results of this research to a wider population, the researcher believes that applying privacy by design for mobile cloud computing is critical for public organizations, users, and private organizations. To conclude, the findings of this study will assist practitioners and researchers, along with managers and policymakers, with the necessary perception when utilizing PbD to preserve privacy and personal data in mobile cloud computing. In future research, a study to inspect the PPDP in MCC classified by individual interests, for example, personal health data, personal financial data, and personal social data is interesting for further research. Furthermore, the results of this research encouraged and supported the usage of PbD to preserve PPDP in mobile cloud computing.

REFERENCES

A Almusaylim, & Jhanjhi. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wireless Personal Communications, 111*(1), 541-564.

Ab Hamid, Sami, & Sidek. (2017). *Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion.* Paper presented at the Journal of Physics: Conference Series.

Abd Al Ghaffar. (2020). Government Cloud Computing and National Security. *Review of Economics and Political Science*.

Abd Razak, Ab Rahman, & Borhan. (2016). Modeling firm resources–enterprise risk management relationships: An empirical finding using PLS-SEM. *World Journal of Entrepreneurship, Management and Sustainable Development*.

Accountants, & Accountants. (2009). Generally Accepted Privacy Principles: CPA and CA Practitioner Version: AICPA/CICA New York, NY.

Adjei, Adams, & Mamattah. (2021). Cloud computing adoption in Ghana; accounting for institutional factors. *Technology in Society, 65*, 101583.

Afandi, Kusyanti, & Wardani. (2017). Analisis hubungan kesadaran keamanan, privasi informasi, dan perilaku keamanan pada para pengguna media sosial Line. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548*, 964X.

Ahmad, Wang, Ullah, & Mahmood. (2018). Reputation-aware trust and privacy-preservation for mobile cloud computing. *IEEE Access, 6*, 46363-46381.

Ahmed, Lee, Su, & Zakari. (2020). Dynamic software updating: a systematic mapping study. *IET Software, 14*(5), 468-481.

Ahn. (2014). User agent to exercise privacy control management in a user-centric identity management system: Google Patents.

Aityan. (2022). Survey Method *Business Research Methodology* (pp. 343-357): Springer.

Ajzen. (1988). Attitudes, personality, and behavior. Homewood, IL, US. *Dorsey Press. http://dx. doi. org/10.1148/radiology, 166*, 3340772.

Ajzen. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Akhtar, Kerim, Perwej, Tiwari, & Praveen. (2021). A Comprehensive Overview of Privacy and Data Security for Cloud Storage. *International Journal of Scientific Research in Science Engineering and Technology*.

Akinde. (2016). Theoretical modelling to explain lecturers' use of educational support systems for teaching in university based library schools in Nigeria: Extending the Technology Acceptance Model (TAM).

Akter, D'Ambra, & Ray. (2011). An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GoF index.

Al-diabat. (2019). Investigating the determinants of college students information security behavior using a validated multiple regression models. *Available at SSRN 3336446*.

Al-Janabi, Al-Shourbaji, Shojafar, & Abdelhag. (2017). *Mobile cloud computing: challenges and future research directions.* Paper presented at the 2017 10th International Conference on Developments in eSystems Engineering (DeSE).

Al-Lozi, & Papazafeiropoulou. (2012). Intention-based models: The theory of planned behavior within the context of IS *Information systems theory* (pp. 219-239): Springer.

Al-Maroof, & Al-Emran. (2018). Students Acceptance of Google Classroom: An Exploratory Study using PLS-SEM Approach. *International Journal of Emerging Technologies in Learning, 13*(6).
Al Khater. (2017). *A model of a private sector organisation's intention to adopt cloud computing in the Kingdom of Saudi Arabia.* University of Southampton.
AlAhmad, Kahtan, Alzoubi, Ali, & Jaradat. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications, 190*, 103152.
Alakbarov, & Alakbarov. (2018). SECURITY AND PRIVACY ISSUES IN MOBILE CLOUD COMPUTING. *Problems of information technology*, 83-91.
Albarq, & Alsughayir. (2013). Examining theory of reasoned action in internet banking using SEM among Saudi consumers. *International journal of marketing practices, 1*(1), 16-30.
Aldholay, Isaac, Abdullah, & Ramayah. (2018). The role of transformational leadership as a mediating variable in DeLone and McLean information system success model: The context of online learning usage in Yemen. *Telematics and Informatics, 35*(5), 1421-1437.
Alguliyev, Aliguliyev, & Abdullayeva. (2019). Privacy-preserving deep learning algorithm for big personal data analysis. *Journal of Industrial Information Integration, 15*, 1-14.
Ali, Hussain, Ali, Hussain, & Murtaza. Analyzing the Impact of Coordination Factors on Construction Project Success in Pakistan Using Partial Least Squares Structural Equation Modeling.
Alnemr, Cayirci, Corte, Garaga, Leenes, Mhungu, Pearson, Reed, Oliveira, Stefanatou, Tetrimida, & Vranaki. (2016). *A Data Protection Impact Assessment Methodology for Cloud* (Vol. 9484).
Ameme, & Yeboah-Boateng. (2016). Internet banking security concerns: an exploratory study of customer behaviors based on health belief model. *Int. J. Emerg. Sci. Eng.(IJESE), 4*(3).
Amini, & Jamil. (2018). *A comprehensive review of existing risk assessment models in cloud computing.* Paper presented at the Journal of Physics: Conference Series.
Angin, Bhargava, Ranchal, Singh, Linderman, Othmane, & Lilien. (2010). *An entity-centric approach for privacy and identity management in cloud computing.* Paper presented at the 2010 29th IEEE symposium on reliable distributed systems.
Anjaneya, Divya, Kumar, Kumar, & Dilip. (2021). *MUTUAL ENTITY AUTHENTICATION PROTOCOL FOR MOBILE CLOUD COMPUTING.* Paper presented at the 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA).
Anwar, He, Ash, Yuan, Li, & Xu. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.
Arpaci. (2019). A hybrid modeling approach for predicting the educational use of mobile cloud computing services in higher education. *Computers in Human Behavior, 90*, 181-187.
Asrani. (2013). Mobile cloud computing. *International Journal of Engineering and Advanced Technology, 2*(4), 606-609.
Azizah, & Puspito. (2021). Satisfaction and Loyalty of Banking Customers in Indonesia. *IPTEK The Journal of Engineering, 6*(3), 63-72.
Bagozzi, & Yi. (1988). On the evaluation of structural equation models. *Journal of the academy of marketing science, 16*(1), 74-94.
Baharon, Shi, & Llewellyn-Jones. (2015). *A new lightweight homomorphic encryption scheme for mobile cloud computing.* Paper presented at the 2015 IEEE

International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

Balaji Raykar, & Sridhar. (2022). *Elicitation of Personal Data Categories for Implementing Data Protection: An Exploratory Study in an Educational Institution.* Paper presented at the 15th Innovations in Software Engineering Conference.

Bansal, Zahedi, & Gefen. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Bellman, Johnson, Kobrin, & Lohse. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

Bender, Cyr, Arbuckle, & Ferris. (2017). Ethics and privacy implications of using the internet and social media to recruit participants for health research: a privacy-by-design framework for online recruitment. *Journal of Medical Internet Research, 19*(4), e104.

Bernsmed. (2016). *Applying privacy by design in software engineering: An European perspective.* Paper presented at the Proc. Second Int. Conf. Advances and Trends in Software Engineering.

Bernsteiner, Ebersberger, & Kilian. (2016). Mobile Cloud Computing for Enterprise Systems: A Conceptual Framework for Research. *International Journal of Interactive Mobile Technologies, 10*(2).

Bhatia, & Verma. (2017). Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues. *The Journal of Supercomputing, 73*(6), 2558-2631.

Bikoro, Wamba, & Kamdjoug. (2018). *Determinants of Cyber Security Use and Behavioral Intention: Case of the Cameroonian Public Administration.* Paper presented at the World Conference on Information Systems and Technologies.

Blume. (2010). Data Protection and Privacy–Basic Concepts in a Changing World. *Scandinavian Studies in Law. ICT Legal Issues, 56*, 151-164.

Brown. (2010). Likert scale examples for surveys. *ANR Program evaluation, Iowa State University, USA*.

Bu, Wang, Jiang, & Liang. (2020). "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management, 53*, 102124.

Burgess. (2013). Computer crimes. *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime*, 1959.

Burmeister, Drews, & Schirmer. (2019). *A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation.* Paper presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences.

Buyya, Yeo, & Venugopal. (2008). *Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities.* Paper presented at the 2008 10th IEEE international conference on high performance computing and communications.

Cao. (2010). In-depth behavior understanding and use: the behavior informatics approach. *Information Sciences, 180*(17), 3067-3085.

Cassidy. (2018). *Thinking Disposition Level-of-Effort Moderates Behavioral Economics of Context-Based Privacy Disclosure Involving Mobile Applications.* Northcentral University.

Cavoukian. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada, 5*, 12.
Cavoukian. (2010). Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach. *Verfügbar online unter http://www. ipc. on. ca/images/Resources/pbd-NEC-cloud. pdf*.
Cavoukian. (2017). Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head: Springer.
Cavoukian. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. *IEEE Consumer Electronics Magazine, 9*(2), 78-82.
Cavoukian, & Chibba. (2018). Start with privacy by design in all big data applications *Guide to big data applications* (pp. 29-48): Springer.
Cavoukian, & Spencer. (2010). The Ontario Health Study's Assessment Centres: A Case Study for "Privacy by Design". *Information and Privacy Commissioner of Ontario: Toronto, ON, Canada*.
Cavoukian, Taylor, & Abrams. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society, 3*(2), 405-413.
Champion, & Skinner. (2008). The health belief model. *Health behavior and health education: Theory, research, and practice, 4*, 45-65.
Chao. (2019). Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. *Frontiers in psychology, 10*, 1652.
Chaubey, & Tank. (2016). Security, privacy and challenges in Mobile Cloud Computing (MCC):-a critical study and comparison. *International Journal of Innovative Research in Computer and Communication Engineering, 4*(2), 1259-1266.
Chen. (2017). Examining Internet Users' Adaptive and Maladaptive Security Behaviors Using the Extended Parallel Process Model.
Chen, & Zhao. (2012). *Data security and privacy protection issues in cloud computing.* Paper presented at the 2012 International Conference on Computer Science and Electronics Engineering.
Cheng, Liu, & Yao. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211.
Chin. (1998a). Commentary: Issues and opinion on structural equation modeling: JSTOR.
Chin. (1998b). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336.
Chin. (2010). How to write up and report PLS analyses. Handbook of Partial Least Squares: Concepts, Methods and Applications, VE Vinzi, WW Chin, J. Henseler, and H. Wang: New York, NY: Springer Verlag.
Chin, Marcolin, & Newsted. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research, 14*(2), 189-217.
Chua. (2018). *Development of an information literacy education model based on school culture mediated by motivation and self-efficacy/Chua Lee Lee.* University of Malaya.
Churchill Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of marketing research, 16*(1), 64-73.
Claar. (2011). The adoption of computer security: an analysis of home personal computer user behavior using the health belief model.

Claar, & Johnson. (2010). Analyzing the adoption of computer security utilizing the Health Belief Model. *Issues in Information Systems, 11*(1), 286-291.
Co-operation, & Development. (2002). *OECD guidelines on the protection of privacy and transborder flows of personal data*: OECD Publishing.
Cohen. (1988). Statistical power analysis for the behavioral sciences New York. *NY: Academic*.
Commission. (2010). A comprehensive approach on personal data protection in the European Union. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions), Brussels, 4*, 2010.
consulting. (2018). General Data Protection Regulation GDPR. from https://gdpr-info.eu/issues/personal-data/
Creswell. (2012). Educational research: planning. *Conducting, and Evaluating*.
Cui, Lai, Wang, & Dai. (2017). Quicksync: Improving synchronization efficiency for mobile cloud storage services. *IEEE Transactions on Mobile Computing, 16*(12), 3513-3526.
Cummings, Jette, & Rosenstock. (1978). Construct validation of the health belief model. *Health education monographs, 6*(4), 394-405.
Cutillo, & Lioy. (2013). *Towards privacy-by-design peer-to-peer cloud computing.* Paper presented at the International Conference on Trust, Privacy and Security in Digital Business.
David, Xavier, & Kathrine. (2017). *A panoramic overview on fast encryption techniques for outsourced data in mobile cloud computing environment.* Paper presented at the 2017 International Conference on Inventive Computing and Informatics (ICICI).
Davis. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.
Davis, Bagozzi, & Warshaw. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science, 35*(8), 982-1003.
Dawson. (2002). *Practical research methods: A user-friendly guide to mastering research techniques and projects*: How to books Ltd.
De Filippi, & McCarthy. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology, 3*(2).
De Wolf, Heyman, & Pierson. (2013). Privacy by design through a social requirements analysis of social network sites form a user perspective *European data protection: Coming of age* (pp. 241-265): Springer.
Deloitte. (2016). Data Privacy in the Cloud: Navigating the New Privacy Regime in a Cloud Environment: Deloitte New York, NY.
Dey, Sampalli, & Ye. (2016). MDA: message digest-based authentication for mobile cloud computing. *Journal of Cloud Computing, 5*(1), 1-13.
Dodel, & Mesch. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior, 68*, 359-367.
Dodiya, & Singh. Towards Categorization of Network Layer Attacks. *International Journal of Computer Applications, 975*, 8887.
Dommeyer, & Gross. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34-51.
Dove. (2018). The EU General Data Protection Regulation: implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics, 46*(4), 1013-1030.

Dyba, Dingsoyr, & Hanssen. (2007). *Applying systematic reviews to diverse study types: An experience report.* Paper presented at the First international symposium on empirical software engineering and measurement (ESEM 2007).
Edwards. (2015). Examining the security awareness, information privacy, and the security behaviors of home computer users.
Ehécatl Morales-Trujillo, García-Mireles, Matla-Cruz, & Piattini. (2019). A Systematic Mapping Study on Privacy by Design in Software Engineering.
Elizabeth, & Lynn. (2014). Belief Systems, religion, and Behavioral economics: New York: Business Expert Press LLC Reisinger, Yv.(2009). International ….
Eltayeb, & Dawson. (2016). Understanding user's acceptance of personal cloud computing: Using the Technology Acceptance Model *Information technology: New generations* (pp. 3-12): Springer.
Esmaeili. (2014). Assessment of users' information security behavior in smartphone networks.
Everson. (2016). Privacy by design: Taking ctrl of big data. *Clev. St. L. Rev., 65*, 27.
Falk, & Miller. (1992). *A primer for soft modeling*: University of Akron Press.
Fatima, & Colomo-Palacios. (2018). Security aspects in healthcare information systems: A systematic mapping. *Procedia Computer Science, 138*, 12-19.
Felix, & Lee. (2019). Systematic literature review of preprocessing techniques for imbalanced data. *IET Software, 13*(6), 479-496.
Fernando, Loke, & Rahayu. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems, 29*(1), 84-106.
Ferreira, & da Silva. (2014). Mobile cloud computing. *Open Journal of Mobile Computing and Cloud Computing, 1*(2), 59-77.
Flores, Srirama, & Paniagua. (2011). *A generic middleware framework for handling process intensive hybrid cloud services from mobiles.* Paper presented at the Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia.
Fornell, & Larcker. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.
Fromholz. (2000). The European Union data privacy directive. *Berk. Tech. LJ, 15*, 461.
Gai, Qiu, Zhao, Tao, & Zong. (2016). Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. *Journal of Network and Computer Applications, 59*, 46-54.
Garlie. (2020). *California Consumer Privacy Act of 2018: A Study of Compliance and Associated Risk.* Utica College.
Gefen, & Straub. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems, 16*(1), 5.
Gefen, Straub, & Boudreau. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information systems, 4*(1), 7.
Gellman. (2009). *Privacy in the clouds: Risks to privacy and confidentiality from cloud computing.* Paper presented at the World privacy forum.
Gellman. (2012). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. World Privacy Forum, 23 February 2009.
Gholami, & Laure. (2016). Security and privacy of sensitive data in cloud computing: a survey of recent developments. *arXiv preprint arXiv:1601.01498*.
Glanz, Rimer, & Viswanath. (2008). *Health behavior and health education: theory, research, and practice*: John Wiley & Sons.
Goyal, & Singh. (2014). Mobile Cloud Computing. *International Journal of Enhanced Research in Science Technology & Engineering, 3*(4), 517-521.

Groenewold, de Bruijn, & Bilsborrow. (2006). *Migration of the Health Belief Model (HBM): Effects of psychosocial and migrant network characteristics on emigration intentions in five countries in West Africa and the Mediterranean Region.* Paper presented at the Annual Meeting of the Population Association of America, Los Angeles, March 30-April 1, 2006.

Grundstrom, Väyrynen, Iivari, & Isomursu. (2019). *Making sense of the general data protection regulation—four categories of personal data access challenges.* Paper presented at the Proceedings of the 52nd Hawaii international conference on system sciences.

Guilloteau, & Venkatesen. (2013). Privacy in Cloud Computing-ITU-T Technology Watch Report March 2012.

Hadar, Hasson, Ayalon, Toch, Birnhack, Sherman, & Balissa. (2018). Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering, 23*(1), 259-289.

Hair. (2009). Multivariate data analysis.

Hair, Anderson, Babin, & Black. (2010). Multivariate data analysis: A global perspective (Vol. 7): Pearson Upper Saddle River: NJ.

Hair, Black, Babin, Anderson, & Tatham. (2006). Multivariate data analysis (Vol. 6): Upper Saddle River, NJ: Pearson Prentice Hall.

Hair Jr, Hult, Ringle, & Sarstedt. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage publications.

Hair Jr, Matthews, Matthews, & Sarstedt. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis, 1*(2), 107-123.

Hair, Ringle, & Sarstedt. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Han, Yang, Wang, Mu, & Liu. (2018). Efficient multifactor two-server authenticated scheme under mobile cloud computing. *Wireless Communications and Mobile Computing, 2018*.

Hanen, Kechaou, & Ayed. (2016). An enhanced healthcare system in mobile cloud computing environment. *Vietnam Journal of Computer Science, 3*(4), 267-277.

Haque, Mahmood, Ahmed, Ali, & Piyal. (2020). Challenges and Opportunities in Mobile Cloud Computing.

Harfoushi. (2017). TRUST MODEL FOR EFFECTIVE CLOUD COMPUTING USAGE: A QUANTITATIVE STUDY. *Journal of Theoretical & Applied Information Technology, 95*(5).

Hartanti, Romadon, Anisah, & Utomo. (2021). *Information Systems Behavior on System Security in the Perspective of "Theory of Reasoned Action".* Paper presented at the 2nd Annual Conference on Social Science and Humanities (ANCOSH 2020).

Harvey, & Lawson. (2009). The importance of health belief models in determining self- care behaviour in diabetes. *Diabetic Medicine, 26*(1), 5-13.

Hassan, & Ismail. (2015). A conceptual model towards information security culture in health informatics *The Malaysia-Japan Model on Technology Partnership* (pp. 187-196): Springer.

Hayes, & Cappa. (2018). Open-source intelligence for risk assessment. *Business Horizons, 61*(5), 689-697.

Hayes, Cappa, & Le-Khac. (2020). An effective approach to mobile device management: security and privacy issues associated with mobile applications. *Digital Business, 1*(1), 100001.

Henseler, Hubona, & Ray. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial management & data systems*.

Henseler, Ringle, & Sarstedt. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science, 43*(1), 115-135.
Henseler, Ringle, & Sinkovics. (2009). The use of partial least squares path modeling in international marketing *New challenges to international marketing*: Emerald Group Publishing Limited.
Henseler, & Sarstedt. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics, 28*(2), 565-580.
Hevner, & Chatterjee. (2010). Design science research in information systems *Design research in information systems* (pp. 9-22): Springer.
Hevner, March, Park, & Ram. (2004). Design science in information systems research. *MIS quarterly*, 75-105.
Hewitt. (2008). ORGs for scalable, robust, privacy-friendly client cloud computing. *IEEE Internet Computing, 12*(5), 96-99.
Hoadley, Xu, Lee, & Rosson. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications, 9*(1), 50-60.
Hong, Thong, Wong, & Tam. (2002). Determinants of user acceptance of digital libraries: an empirical examination of individual differences and system characteristics. *Journal of management information systems, 18*(3), 97-124.
Hosain, & Liu. (2020). LinkedIn for Searching Better Job Opportunity: Passive Jobseekers' Perceived Experience. *The Qualitative Report, 25*(10), 3719-3732.
Hosseini, Turhan, & Mäntylä. (2018). A benchmark study on the effectiveness of search-based data selection and feature selection for cross project defect prediction. *Information and Software Technology, 95*, 296-312.
Huang, & Wu. (2017). *Mobile cloud computing: foundations and service models*: Morgan Kaufmann.
Huang, Zhou, Xu, Xing, & Zhong. (2011). *Secure data processing framework for mobile cloud computing.* Paper presented at the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).
Hulland. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic management journal, 20*(2), 195-204.
Humaidi, & Balakrishnan. (2012). *The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework.* Paper presented at the 2nd International Conference on Management and Artificial Intelligence IPEDR.
Humaidi, & Balakrishnan. (2015). The Moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science, 28*(2), 70-92.
Hussain, Turab Mirza, Rasool, Hussain, & Kaleem. (2019). Spam review detection techniques: A systematic literature review. *Applied Sciences, 9*(5), 987.
Hustinx. (2010). Privacy by design: delivering the promises. *Identity in the Information Society, 3*(2), 253-255.
i-scoop. (2016). General Data Protection Regulation: the online guide to the EU GDPR.
Ikram, Fiaz, Mahmood, Ahmad, & Ashfaq. (2021). Internal Corporate Responsibility as a Legitimacy Strategy for Branding and Employee Retention: A Perspective of Higher Education Institutions. *Journal of Open Innovation: Technology, Market, and Complexity, 7*(1), 52.
Ikram, Javed, Rizwan, Abid, Crichigno, & Srivastava. (2021). *Mobile cloud computing framework for securing data.* Paper presented at the 2021 44th International Conference on Telecommunications and Signal Processing (TSP).

Islam, & Iannella. (2011). *Privacy by design: Does it matter for social networks?* Paper presented at the IFIP PrimeLife International Summer School on Privacy and Identity Management for Life.
Jaidka, Khoo, & Na. (2013). *Literature review writing: how information is selected and transformed.* Paper presented at the Aslib Proceedings.
Janadari, Sri Ramalu, & Wei. (2016). Evaluation of measurment and structural model of the reflective model constructs in PLS–SEM.
JEEVAN, HALMANDGE, & PUSHPALATHA. (2014). Mobile Cloud Computing Service Models: A User-Centric Approach.
Jokonya. (2017). Critical literature review of theory of planned behavior in the information systems research. *DEStech Transactions on Computer Science and Engineering*(ameit).
Jones, Jensen, Scherr, Brown, Christy, & Weaver. (2015). The health belief model as an explanatory framework in communication research: Exploring parallel, serial, and moderated mediation. *Health communication, 30*(6), 566-576.
Juárez, & Cedillo. (2017). *Security of mobile cloud computing: A systematic mapping study.* Paper presented at the 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM).
Jung. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior, 70*, 303-309.
Jusob, George, & Mapp. (2017). Exploring the need for a suitable privacy framework for mHealth when managing chronic diseases. *Journal of Reliable Intelligent Environments, 3*(4), 243-256.
Kamis. (2021). The SmartPLS Analyzes Approach in Validity and Reliability of Graduate Marketability Instrument. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(3), 829-841.
Kassem, Khoiry, & Hamzah. (2020). Assessment of the effect of external risk factors on the success of an oil and gas construction project. *Engineering, Construction and Architectural Management*.
Kayaalp. (2018). Patient privacy in the era of big data. *Balkan medical journal, 35*(1), 8.
Keele. (2007). Guidelines for performing systematic literature reviews in software engineering: Citeseer.
Khan, Kiah, Khan, & Madani. (2013). Towards secure mobile cloud computing: A survey. *Future Generation Computer Systems, 29*(5), 1278-1299.
Kim, & Park. (2012). Development of a health information technology acceptance model using consumers' health behavior intention. *Journal of medical Internet research, 14*(5), e133.
Kitchenham, & Brereton. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology, 55*(12), 2049-2075.
Kitchenham, & Charters. (2007). Guidelines for performing systematic literature reviews in software engineering.
Kolkowska. (2015). *Privacy principles in design of smart homes systems in elderly care.* Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust.
Kolkowska, & Kristofferson. (2016). *Privacy by design principles in design of new generation cognitive assistive technologies.* Paper presented at the IFIP International Conference on ICT Systems Security and Privacy Protection.
Koloseni. (2017). *The practice of information security: An analysis of government employees in Tanzania using the Health Belief Model (HBM).* UTAR.

Koloseni, Lee, & Gan. (2019). Understanding Information Security Behaviours of Tanzanian Government Employees: A Health Belief Model Perspective. *International Journal of Technology and Human Interaction (IJTHI), 15*(1), 15-32.
Kosar, Bohra, & Mernik. (2016). Domain-specific languages: A systematic mapping study. *Information and Software Technology, 71*, 77-91.
Kroener, & Wright. (2014). A strategy for operationalizing privacy by design. *The Information Society, 30*(5), 355-365.
Kronenfeld, & Glik. (1991). Perceptions of risk: Its applicability in medical sociological research. *Research in the Sociology of Health Care, 9*, 307-334.
Kucharczyk, & Joachymczyk. (2021). The right to privacy and personal data protection in the age of new technologies. *Scientific Journal of Bielsko-Biala School of Finance and Law, 25*(4), 23-28.
Kulkarni, Khanai, & Bindagi. (2016). *Security frameworks for mobile cloud computing: A survey.* Paper presented at the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).
Kumar, Raj, & Jelciana. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science, 125*, 691-697.
Lada, Tanakinjal, & Amin. (2009). Predicting intention to choose halal products using theory of reasoned action. *International journal of Islamic and Middle Eastern finance and management*.
Lah. (2008). Are ip addresses personally identifiable information. *ISJLP, 4*, 681.
Landau, Cohen, Gordon, & Nissim. (2020). Mind your privacy: Privacy leakage through BCI applications using machine learning methods. *Knowledge-Based Systems, 198*, 105932.
Langheinrich. (2001). *Privacy by design—principles of privacy-aware ubiquitous systems.* Paper presented at the International conference on Ubiquitous Computing.
Le Métayer. (2010). Privacy by design: a matter of choice *Data protection in a profiled world* (pp. 323-334): Springer.
Le Vinh. (2017). *Security and trust in mobile cloud computing.* Paris, CNAM.
Lee, Hsu, Chang, & Cheng. (2016). *Integrating TRA and toe Frameworks for Cloud ERP Switching Intention by Taiwanese Company.* Paper presented at the PACIS.
Li, Rahulamathavan, Conti, & Rajarajan. (2015). Robust access control framework for mobile cloud computing network. *Computer Communications, 68*, 61-72.
Liang, & Xue. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems, 11*(7), 394-413.
Likert. (1932). A technique for the measurement of attitudes. *Archives of psychology*.
Litwin. (1995). *How to measure survey reliability and validity* (Vol. 7): Sage publications.
Liu, & Ma. (2006). Perceived system performance: a test of an extended technology acceptance model. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 37*(2-3), 51-59.
Madden, Ellen, & Ajzen. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin, 18*(1), 3-9.
Mai. (2016). Big data privacy: The datafication of personal information. *The Information Society, 32*(3), 192-199.
Malhotra, & Galletta. (1999). *Extending the technology acceptance model to account for social influence: Theoretical bases and empirical validation.* Paper presented

at the Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers.
Malik, Akram, Gill, Pervaiz, & Malik. (2021). EFFORT: Energy efficient framework for offload communication in mobile cloud computing. *Software: Practice and Experience, 51*(9), 1896-1909.
Malik, Wani, & Rashid. (2018). CLOUD COMPUTING-TECHNOLOGIES. *International Journal of Advanced Research in Computer Science, 9*(2).
Mantelero. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review, 32*(2), 238-255.
Maurushat. (2019). *Ethical Hacking*: University of Ottawa Press.
Mikhail, & Petro- Nustas. (2001). Transcultural adaptation of Champion's health belief model scales. *Journal of Nursing Scholarship, 33*(2), 159-165.
Mollah, Azad, & Vasilakos. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications, 84*, 38-54.
Momani, & Jamous. (2017). The evolution of technology acceptance theories. *International Journal of Contemporary Computer Research (IJCCR), 1*(1), 51-58.
Momeni. (2015). A survey of mobile cloud computing: advantages, challenges and approaches. *InternationalJournal of Computer Science and Business Informatics, 15*(4), 14-28.
Mulligan, Freeman, & Linebaugh. (2019). *Data protection law: an overview.* Paper presented at the R45631. Congressional Research Service. https://crsreports. congress. gov/product/pdf.
Naik, & Sarma. (2013). A Framework for Mobile Cloud Computing. *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), 3*(1), 1-12.
Nawrocki, Pajor, Sniezynski, & Kolodziej. (2022). Modeling adaptive security-aware task allocation in mobile cloud computing. *Simulation Modelling Practice and Theory*, 102491.
Nayyar. (2019). *Handbook of Cloud Computing: Basic to Advance research on the concepts and design of Cloud Computing*: BPB Publications.
Ng, Kankanhalli, & Xu. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.
Ng, & Xu. (2007). Studying users' computer security behavior using the health belief model. *PACIS 2007 Proceedings*, 45.
Nunnally. (1978). *Psychometric Theory: 2d Ed*: McGraw-Hill.
ODERO. (2021). *FRAMEWORK FOR ADOPTION OF CLOUD COMPUTING BY SMALL AND MEDIUM-SIZED ENTERPRISES IN MERU COUNTY.* KeMU.
Odusote. (2021). Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation. *Beijing Law Review, 12*(4), 1284-1298.
Oh, Stackpole, Cummins, Gonzalez, Ramachandran, & Lim. (2012). *Best security practices for android, blackberry, and iOS.* Paper presented at the 2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT).
Olushola, & Abiola. (2017). The efficacy of technology acceptance model: A review of applicable theoretical models in information technology researches. *Journal of Research in Business and Management, 4*(11), 70-83.

Onega. (2000). Education theories, models and principles applied to community and public health nursing. *Community and Public Health Nursing; Stanhope, M., Lancaster, J., Eds*, 266-283.
Onumo, Ullah-Awan, & Cullen. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems (TMIS), 12*(2), 1-29.
Opitz, Langkau, Schmidt, & Kolbe. (2012). *Technology acceptance of cloud computing: empirical evidence from German IT departments.* Paper presented at the 2012 45th Hawaii International Conference on System Sciences.
Organization. (2021). The protection of personal data in health information systems-principles and processes for public health: World Health Organization. Regional Office for Europe.
Orji, Vassileva, & Mandryk. (2012). Towards an effective health interventions design: an extension of the health belief model. *Online journal of public health informatics, 4*(3).
Otieno, Liyala, Odongo, & Abeka. (2016). Theory of reasoned action as an underpinning to technological innovation adoption studies.
Pagallo. (2021). On the principle of privacy by design and its limits: Technology, ethics and the rule of law *Italian Philosophy of Technology* (pp. 111-127): Springer.
Pearson. (2013). Privacy, security and trust in cloud computing *Privacy and security for cloud computing* (pp. 3-42): Springer.
Petersen, Feldt, Mujtaba, & Mattsson. (2008). *Systematic mapping studies in software engineering.* Paper presented at the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12.
Petrić, & Czárl. (2003). Validating a writing strategy questionnaire. *System, 31*(2), 187-215.
Petter, Straub, & Rai. (2007). Specifying formative constructs in information systems research. *MIS quarterly*, 623-656.
Phinyomark, N Khushaba, & Scheme. (2018). Feature extraction and selection for myoelectric control based on wearable EMG sensors. *Sensors, 18*(5), 1615.
Polit, & Beck. (2004). *Nursing research: Principles and methods*: Lippincott Williams & Wilkins.
Prachaseree, Ahmad, & Isa. (2021). Applying Theory Elaboration for Theory of Reasoned Action (TRA) and Its Extensions. *GIS Business, 16*(2), 35-57.
Purtova. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innov. Technol. 10 (1), 40–81 (2018).
Purtova. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innov. Technol. 10 (1), 40–81 (2018).
Puspita, Tamtomo, & Indarto. (2017). Health belief model for the analysis of factors affecting hypertension preventive behavior among adolescents in Surakarta. *Journal of Health Promotion and Behavior, 2*(2), 183-196.
Qayyum. (2020). A Critical Survey on Privacy Prevailing in Mobile Cloud Computing: Challenges, State of the Art Methods and Future Directions. *Rida Qayyum," A Critical Survey on Privacy Prevailing in Mobile Cloud Computing: Challenges, State of the Art Methods and Future Directions", International Journal of Wireless and Microwave Technologies (IJWMT), 10*(6), 36-46.
Qi, & Gani. (2012). *Research on mobile cloud computing: Review, trend and perspectives.* Paper presented at the 2012 second international conference on digital information and communication technology and it's applications (DICTAP).

Quick, & Choo. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation, 10*(3), 266-277.
Quick, & Choo. (2014). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications, 40*, 179-193.
Rahimi, Ren, Liu, Vasilakos, & Venkatasubramanian. (2014). Mobile cloud computing: A survey, state of art and future directions. *Mobile Networks and Applications, 19*(2), 133-143.
Ranchal, Bhargava, Othmane, Lilien, Kim, Kang, & Linderman. (2010). *Protection of identity information in cloud computing without trusted third party.* Paper presented at the 2010 29th IEEE symposium on reliable distributed systems.
Ratten. (2017). Mobile cloud computing: innovation and creativity perspectives. *International Journal of Technology Marketing, 12*(1), 60-70.
Rayapuri. (2018). *A Survey of Security and Privacy in Mobile Cloud Computing.* Western Michigan University.
Raygor. (2016). *The theory of planned behavior: Understanding consumer intentions to purchase local food in Iowa.* Iowa State University.
Ringle, Da Silva, & Bido. (2015). Structural equation modeling with the SmartPLS. *Bido, D., da Silva, D., & Ringle, C.(2014). Structural Equation Modeling with the Smartpls. Brazilian Journal Of Marketing, 13*(2).
Riyadi. (2021). Data Privacy in the Indonesian Personal Data Protection Legislation.
Rosenstock. (1974). Historical origins of the health belief model. *Health education monographs, 2*(4), 328-335.
Ross, CISA, & AFBCI. (2019). Information Security Matters: Un-Privacy by Design.
Ruiter, & Warnier. (2011). Privacy regulations for cloud computing: Compliance and implementation in theory and practice *Computers, privacy and data protection: an element of choice* (pp. 361-376): Springer.
Ryan. (2011). Cloud computing privacy concerns on our doorstep. *Communications of the ACM, 54*(1), 36-38.
Sarstedt, Ringle, & Hair. (2017). Partial least squares structural equation modeling. *Handbook of market research, 26*(1), 1-40.
Sawilowsky. (2009). New effect size rules of thumb. *Journal of Modern Applied Statistical Methods, 8*(2), 26.
Schaale. (2014). How cloud providers are adopting privacy by design. *Journal of Internet Regulation*.
Schymik, & Du. (2017). *Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model.* Paper presented at the Proceedings of the Conference on Information Systems Applied Research ISSN; ISCAP: São Mamede de Infesta, Portugal.
Schymik, Du, & Kalafut. (2019). Location Based Services and the Health Belief Model Based Investigation of Student Intentions and Behaviors.
Scott. (2020). *A Correlation Study of Smartwatch Adoption and Privacy Concerns with US Consumers Using the UTAUT2.* Colorado Technical University.
Sekyere. (2015). Studying Information Security Behaviour among Students in Tertiary Institutions.
Semantha, Azam, Yeo, & Shanmugam. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics, 9*(3), 452.
Sha, Xie, Tan, Bai, Li, & Liu. (2017). Assessing the impacts of human activities and climate variations on grassland productivity by partial least squares structural equation modeling (PLS-SEM). *Journal of Arid Land, 9*(4), 473-488.
Shah. (2019). Green human resource management: Development of a valid measurement scale. *Business Strategy and the Environment, 28*(5), 771-785.

Shana, & Abulibdeh. (2017). Cloud Computing Issues for Higher Education: Theory of Acceptance Model. *International Journal of Emerging Technologies in Learning, 12*(11).
Shen, Qin, Yu, Hao, & Hu. (2018). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *IEEE Transactions on Information Forensics and Security, 14*(2), 331-346.
Shin, Kim, & Kwon. (2016). Study on Personal Information Protection Behavior in Social Network Service Using Health Belief Model. *Journal of the Korea Institute of Information Security & Cryptology, 26*(6), 1619-1637.
Shirazi, Seddighi, & Iqbal. (2017). *Cloud computing security and privacy: an empirical study.* Paper presented at the International Conference on Human-Computer Interaction.
Shmueli, Sarstedt, Hair, Cheah, Ting, Vaithilingam, & Ringle. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing*.
Shriwas, Gupta, & Sinhal. (2012). Comparative Study of Cloud Computing and Mobile Cloud Computing. *MEDHA-2012 Proceedings published by International Journal of Computer Applications (IJCA.)*.
Sindhu, & Meshram. (2012). Digital forensic investigation tools and procedures. *International Journal of Computer Network and Information Security, 4*(4), 39.
Singh, & Dhiman. (2021). A survey on cloud computing approaches. *Materials Today: Proceedings*.
Skendžić, Kovačić, & Tijan. (2018). *General data protection regulation—Protection of personal data in an organisation.* Paper presented at the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
Somula, & Sasikala. (2018). A survey on mobile cloud computing: mobile computing+ cloud computing (MCC= MC+ CC). *Scalable Computing: Practice and Experience, 19*(4), 309-337.
Stallings. (2006). *Cryptography and network security, 4/E*: Pearson Education India.
Stantchev, Prieto-González, & Tamm. (2015). Cloud computing service for knowledge assessment and studies recommendation in crowdsourcing and collaborative learning environments based on social network analysis. *Computers in Human Behavior, 51*, 762-770.
Stergiou, Psannis, Kim, & Gupta. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964-975.
Stevens. (1946). On the theory of scales of measurement.
Taherdoost. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. *How to test the validation of a questionnaire/survey in a research (August 10, 2016)*.
Tang, Hsiao, Tu, Hwang, & Wang. (2021). Factors influencing university teachers' use of a mobile technology-enhanced teaching (MTT) platform. *Educational Technology Research and Development, 69*(5), 2705-2728.
Tarkang, & Zotor. (2015). Application of the health belief model (HBM) in HIV prevention: A literature review. *Central African Journal of Public Health, 1*(1), 1-8.
Tavallaee, Shokouhyar, & Samadi. (2017). The combined theory of planned behaviour and technology acceptance model of mobile learning at Tehran universities. *International Journal of Mobile Learning and Organisation, 11*(2), 176-206.
Taylor, & Todd. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International journal of research in marketing, 12*(2), 137-155.

Tehseen, Sajilan, Gadar, & Ramayah. (2017). Assessing cultural orientation as a reflective-formative second order construct-a recent PLS-SEM approach. *Review of Integrative Business and Economics Research, 6*(2), 38.
Tenenhaus, Vinzi, Chatelin, & Lauro. (2005). PLS path modeling. *Computational statistics & data analysis, 48*(1), 159-205.
Tikkinen-Piri, Rohunen, & Markkula. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.
Tongco. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications, 5*, 147-158.
Tubay. (2021). Students' Use of Cloud Storage in Their Studies: A Case of a Private University in the Philippines. *Journal of Education and e-Learning Research, 8*(1), 16-25.
Tumusiime. (2004). *Perceived benefits of, barriers and helpful cues to physical activity among tertiary institution students in Rwanda.* University of the Western Cape.
Vaile, Kalinich, Fair, & Lawrence. (2013). Data Sovereignty and the Cloud: A Board and Executive Officer's Guide. *UNSW Law Research Paper*(2013-84).
Vasantha, & Harinarayana. (2016). *Online survey tools: A case study of Google Forms.* Paper presented at the National Conference on" Scientific, Computational & Information Research Trends in Engineering, GSSS-IETW, Mysore.
Vatka. (2019). INFORMATION BEHAVIOUR and DATA SECURITY: Health Belief Model Perspective.
Venkatesh, & Eastaff. (2018). A study of data storage security issues in cloud computing. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(1), 1741-1745.
Wallace, Blake, Parham, & Baldridge. (2003). Development and content validation of family practice residency recruitment questionnaires. *FAMILY MEDICINE-KANSAS CITY-, 35*(7), 496-498.
Wang. (2011). *Mobile cloud computing.*
Wang, & Jin. (2019). An Overview of Mobile Cloud Computing for Pervasive Healthcare. *IEEE Access, 7*, 66774-66791.
Weishäupl, Yasasin, & Schryen. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807-823.
Wetzels, Odekerken-Schröder, & Van Oppen. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS quarterly*, 177-195.
Wilkinson, & Birmingham. (2003). *Using research instruments: A guide for researchers*: Psychology Press.
Williams, Wynn, Madupalli, Karahanna, & Duncan. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing (JOEUC), 26*(3), 23-46.
Witti, & Konstantas. (2018). IOT and Security-Privacy Concerns: A Systematic Mapping Study. *International Journal of Network Security & Its Applications (IJNSA) Vol, 10*.
Wohlin, Runeson, Höst, Ohlsson, Regnell, & Wesslén. (2012). Experimentation in software engineering, vol. 9783642290: Springer.
Wong. (2007). Data protection online: alternative approaches to sensitive data. *J. Int'l Com. L. & Tech., 2*, 9.
Wong. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*(1), 1-32.

Wong. (2016). Mediation analysis, categorical moderation analysis, and higher-order constructs modeling in Partial Least Squares Structural Equation Modeling (PLS-SEM): A B2B Example using SmartPLS. *Marketing Bulletin, 26*.
Xhafaj, Qendraj, Xhafaj, & Halidini. (2021). Analysis and Evaluation of Factors Affecting the Use of Google Classroom in Albania: A Partial Least Squares Structural Equation Modelling Approach.
Yacob, Lee, Nodeson, Yee, & Fared. (2017). Cleaner technologies adoption: Outcomes of E&F manufacturing SMEs sustainability.
Yahya. (2017). *A security framework to protect data in cloud storage.* University of Southampton.
YAJID. (2017). AN ARIES ALGORITHM FOR OPTIMAL DATA RECOVERY IN DATABASE SERVER.
Yanisky-Ravid, & Hallisey. (2019). Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency Via Auditing, Certification, and Safe Harbor Regimes. *Fordham Urb. LJ, 46*, 428.
Yap. (2022). The Mediating Effects of Perceived Value Between the Relationship of Social Media Marketing and Purchase Intention.
Young, Carpenter, & McLeod. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research, 2*(1), 8.
Yuen, Li, Ma, & Wang. (2020). The effect of emotional appeal on seafarers' safety behaviour: An extended health belief model. *Journal of Transport & Health, 16*, 100810.
Zhou, & Huang. (2012). *Efficient and secure data storage operations for mobile cloud computing.* Paper presented at the 2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm).
Zukarnain. (2021). Online Identity Theft, Security Issues, and Reputational Damage.