# EXAMINING TRUST AS A PREDICTOR OF ADOPTING FEDERATED IDENTITY MANAGEMENT IN U.S. BUSINESS

by

Bunmi Samuel

LAWRENCE NESS, PhD, Faculty Mentor and Chair

GLENN BOTTOMLY, PhD, Committee Member

WENBIN LUO, PhD, Committee Member

Rhonda Capron, EdD, Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

August 2018

# Abstract

This quantitative predictive study involved investigating the extent to which the dimensions of trust (security, privacy, and perceived risk) relate to behavioral intentions to adopt federated identity management (FIM), in conjunction with the unified theory of acceptance and use of technology (UTAUT) constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business. Although UTAUT is an ideal choice for studying technology innovation adoption, the model still receives criticism from researchers. There is also skepticism among organizational leaders about accepting federated identity, despite its potential business value. Trust is considered the most crucial part of the identity management process, but it has not received much attention as part of FIM. The study involved using Qualtrics, an online survey company, for collecting data to obtain a quantitative description of trends, attitudes, or opinions of information technology decision-makers in U.S. business. The study involved analyzing the data and testing the hypotheses using structural equation modeling and multiple regression analysis. The result of the structural equation modeling revealed that security, privacy concern, and perceived risk predict trust at statistically significant level (p < .001) and the hierarchical multiple regression result indicated that the data were a good fit for the model (R = .726) and that the addition of trust in the equation improved the model by 5%. The researcher observed statistical significance ($p < .05$) among all the independent variables about the dependent variable. The result of the individual predictors was that trust had the highest predictability at $p < .001$, followed by performance expectancy, which had $p < .005$. Data analysis revealed the ability to use trust to predict the adoption of FIM in U.S. business is statistically significant. The results of the research contributed to the body of literature on the adoption of FIM by IT decision maker and provide scholars a foundation for further studies

using, for example, the extensions of UTAUT2 to provide a more in-depth understanding or individual's perception of the phenomenon. The results derived from the analysis of data may be valuable to IT decision makers interested in adopting FIM as a practice in their organization. Understanding what influence that contributes to IT decision maker to adopt new technologies in general, and especially the factors that influence the adoption of FIM will help the organizations define policies and practices that allow businesses to maximize the benefits of FIM to their organization.

## Dedication

This dissertation is dedicated to my creator for giving me the opportunity, grace, and resources to complete this project. I also dedicated this dissertation to my beautiful, lovely and darling wife Olusola Samuel and my little boy Wonderful Samuel. I thank you for always being there for me. Your support and encouragement cannot be quantified. I attributed this achievement to my parents for bringing me to life and for the value system they gave to me. I am forever grateful.

# Acknowledgments

I will like to thank Mr. Olu Ajayi and Dr. Kelly Regal at the Federal Motor Carrier Safety Administration for the support they rendered throughout my academic journey. I wish to thank Dr. Sam Ogunbo, Dr. Jide Odubiyi and Mr. Ayodele Opadina for their support and beautiful words of encouragement. I am also indebted for the incredible support I received throughout my dissertation from my mentor and faculty chair Dr. Lawrence Ness. You provided me with intellectual, practical, and emotional support from the conception to the completion of this study. Your quick response and thought-provoking and valuable feedback were very much appreciated. You are indeed a Godsend. I also wanted to thank Dr. Glen Bottomly and Dr. Wenbin Luo, my committee members, for your continued support and contribution to the success of my dissertation. My special thanks go to Dr. Steven Brown for responding to my questions, particularly when I was searching for the topic.

I would be ungrateful if I did not acknowledge the contributions of all my professors in my academic program, including the residency courses. You made my dream a reality. Lastly, I would like to thank my employer, Noblis NSP, for the financial support they rendered through the Education Assistance Program. I will forever be grateful.

# Table of Contents

## List of Tables

## List of Figures

# CHAPTER 1. INTRODUCTION

## Background of the Problem

The emergence of information technology (IT) has transformed practically all aspects of human creation. In the mid-1990s, the IT revolution changed the manner in which business transactions took place between individuals and enterprises (Gangopadhyay, Nishimura, & Pal, 2016; Haumont, NguyenBa, & Modi, 2017). Information technology is a crucial instrument for increasing the competitiveness of a country's economy (Oliveira & Martins, 2011). Numerous researchers have indicated that the development of advanced IT innovation will significantly improve employees' interaction, participation, and collaboration (Jirotka, Lee, & Olson, 2013; Sandoval-Almazán & Gil-Garcia, 2012). Information technology innovation also improves employees' work performance and productivity (Devaraj, Ow, & Kohli, 2013; Kleis, Chwelos, Ramirez, & Cockburn, 2012).

In the last 50 years, the password has taken over human-computer authentication despite consensus among researchers that there is a need to develop more secure and user-friendly authenticated solutions (Bonneau, Herley, Van Oorschot, & Stajano, 2015). The password is the most dominant form of authentication (Petsas, Tsirantonakis, Athanasopoulos, & Ioannidis, 2015). Nonetheless, password-based protection is inflicted with problems (Katalov, 2015). Many employees feel frustrated when they need to access a myriad of organization resources over the Internet to perform their daily activities, often with different usernames and passwords (Parkin, Driss, Krol, & Sasse, 2015). The management and control of employee identity information have become a daunting task due to the complexity and fragmented nature of organizations' identity information (Parkin et al., 2015; Stobert & Biddle, 2015). The first-generation identity solution was decentralized, and organizational leaders distributed identity information across many different systems. Managing the distributed access management systems is challenging. Burgeoning demand for the Internet as a means of sharing and managing enterprise resources has caused an increased burden on verification and authorization processes. In addition to employees, online service providers are also struggling to devise a means to secure, protect, and verify the privacy of their consumers. The default method requires individual consumers to register and create an account each time they need a new service. The decentralization of account management is another burden placed on service providers to maintain and track users' login activities.

At the start of the 21st century, various technology researchers, academia, and organizational leaders had conducted a variety of studies to advance and centralize the account management process. The primary goal has been to develop a secure cross-domain and flexible solution that combines single sign-on (SSO) services with authorization based on an exchange of identity-related assertions across security domains (Lynch, 2011) using a concept known as federated identity management (FIM). Federated identity management is a model that allows employees in companies with several different technologies, processes, policies, and standards to share their applications using the same login credential (Jensen, 2012). Federated identity management is a promising, centralized, and automated approach to facilitate secure access to enterprise resources among cooperating partners in mixed information technology settings (Jensen, 2012; see Figure 1). Thibeau (2016) defined FIM as "agreements, standards, and technologies that enable portability of identities, identity attributes, and entitlements across multiple enterprises and numerous applications supporting thousands, even millions, of users" (p.2). One of the benefits of trust relationship associated with the identity was that an employee could leverage on FIM to access services across the federation.

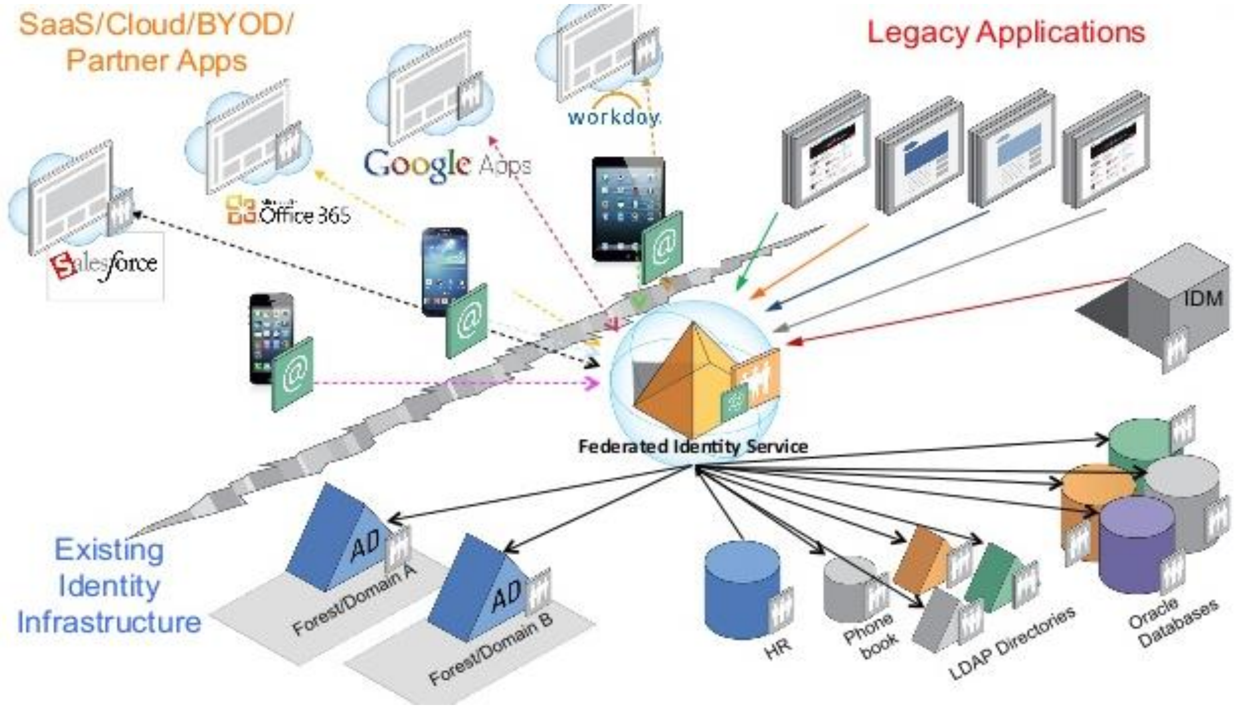


*Figure 1*. Federal identity management. Reprinted from Creating a Federated Identity for ABAC and WebAccess Management (p.7), by W. Ellery and D. Lores, 2014, *Radiant Logic*. Used with permission.

The introduction of FIM systems to business processes offers economic advantages and convenience to the organizations and their subscribers in the form of administration and provisioning cost reduction (Chadwick, Siu, Lee, Fouillat, & Germonville, 2014; Kurowski, 2015). Instead of enrolling external users into an organization's internal identity systems, FIM can enable organizational leaders to offload the cost of administrating these users to their business partner companies (Chadwick et al., 2014). Due to the cooperation that exists in sharing identity information between various partners, multiple subscribers can share a single application resulting in cost savings and resource consolidation (Chadwick et al., 2014). Federated identity management also reduces the administrative burden and elimination of wasted time and costs incurred in password resets, which yields increased productivity for participants.

The primary function of the data governance is to enhance and maintain high-quality data throughout the complete lifecycle. Because organizational leaders rely on timely and accurate data to make a decision, the introduction of FIM has helped improve the quality of organization data. Organizational leaders can store and access updated data in a central location rather than in a distributed environment. Bertino, Martino, Paci, Squicciarini, Martino & Squicciarini (2010) argue that one of the benefits of FIM was that identity information could be made available on demand, up-to-date and consistent with a low delay in a distributed environment compared to a scenario where user data is stored and maintained several places. Other researchers presented a similar view that FIM moved the administrative burden away from the service provider to the identity provider (Han, Mu, Susilo, & Yan, 2010; Hoellrigl, Dinger & Hartenstein, 2010).

Federated identity management simplifies the complex users account management process, improves security and lowers the risk associated with multiple logins and also improves the ability to protect the privacy of users by minimizing information disclosure through the efficient control of user access to information sharing. The organization data steward determines and authorizes users, the data usage and the rules and processes that impact the data and its use. Federated identity management can also eliminate the need to create new accounts to access new systems or applications. Users can benefit from FIM, as they will be able to access any organization’s applications without having to manage logins for each application. Several studies agree the use of FIM will improve privacy information of the subscribers (Jensen, 2011). For example, Grassi & Lefkovitz (2015) believed the main motivating factor of FIM is to enhance user convenience and privacy, while Bertino et al. (2010) and Ahn (2016) claimed that FIM can facilitate users to exercise privacy control management over user identities or what information sent to or managed  by the identity provider.

Federated identity management can improve users' experience by providing an SSO to multiple applications help to ensure compliance with corporate policies and provides a means of provisioning and de-provisioning user access across an entire enterprise.   One of the most significant benefits of FIM is that it is a cross-domain SSO solution that facilitates cooperation among business partners to realize their business goals through cost reduction.

Despite the benefits of FIM, consumers' attitude toward adopting this innovative technology has been slow for several reasons (AlQatan, Singh, & Ahmad, 2012). Researchers have yet to determine the effect of trust on IT decision makers' perception of FIM and have not revealed if there are statistically significant variances in levels of trust that affect IT decision makers' choosing to adopt FIM.

## Statement of the Problem

Despite the business value of adopting FIM becoming well-known within the IT community, the adoption of such technology still faces numerous challenges (Arias-Cabarcos, Almenárez-Mendoza, Marín-López, Díaz-Sánchez, & Sánchez-Guerrero, 2012). What is lacking in scholarly literature are studies that describe the adoption of FIM including how the constructs of the trust factors affect the IT decision maker in US business to adopt the new technology. Trust is a crucial part of the identity management process, and it is one aspect of the research challenges relating to FIM adoption that have remained unresolved (Esteva-Armida & Rubio-Sanchez, 2014). The issue of trust emerges due to an increased need for security and privacy and an increase in perceived risk arising from organization leaders distributing and transmitting sensitive information across various domains using loosely coupled network protocols (Maler & Reed, 2008). Researchers have shown that trust is the most significant obstacle that prevents many IT decision makers from adopting FIM (Odeyinde, 2014; Satchell, Shanks, Howard, & Murphy, 2011; Venkatesh, Morris, Davis, & Davis, 2003; Venkatesh, Thong, & Xu, 2012).

## Purpose of the Study

The purpose of this quantitative correlational research was to investigate the extent to which the dimensions of trust (security, privacy, and perceived risk) relate to behavioral intentions to adopt FIM, as in conjunction with the unified theory of acceptance and use of technology (UTAUT) constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business. The independent variables were trust, security, privacy, perceived risk, performance expectancy, effort expectancy, social influence, and facilitating conditions. Creswell (2009) defined an independent variable as a variable that stands alone, and that determines the values of the dependent variable. Behavioral intention to adopt FIM is a dependent variable and was the measured variable in this study.

The goal of this study was to advance the UTAUT body of knowledge and extend the application of the UTAUT2 model to FIM. The original UTAUT model developed by Venkatesh et al. (2003) consisted of four constructs and four moderating factors. Although such models explain much of the variance, however, trust (security, privacy, and perceived risk) were overlooked or have received inadequate attention in the initial UTAUT model (Im, Kim, & Han, 2008). Researchers have shown trust (security, privacy, and perceived risk) are the most crucial factors to consider in technology acceptance (Lee, Kim, & Song, 2010). In this study, the researcher examined the relationship between trust (security, privacy, and perceived risk) and the constructs of UTAUT. The research provided an understanding of how trust (security, privacy, and perceived risk) in conjunction with the original UTAUT core constructs influence adoption (Lee et al., 2010; Venkatesh et al., 2012).

## Significance of the Study

This study is essential to understanding the adoption of FIM technology from a theoretical perspective, as it provides information about the new factors not considered in the UTAUT. Trust (security, privacy, and perceived risk) of FIM have become a research domain that has enticed massive investment in industries (Alkhalifah & Amro, 2017; Ghazizadeh, Zamani, Ab Manan, & Pashang, 2012; Lee et al., 2010). Several researchers have investigated issues that might affect FIM (Alkhalifah & Amro, 2017; Ghazizadeh et al., 2012; Lee et al., 2010). The quest for a better understanding of FIM had a practical application for U.S. businesses, such as the Clinger-Cohen Act of 1996, the Health Insurance Portability and Accountability Act of 1996, and the Security and Exchange Commission demand the highest level of security and privacy of data. This study also equips the IT decision makers with sufficient information to make an informed adoption decision about FIM. The findings support the reliability of the quantitative, nonexperimental research methodology to predict the likelihood of technology adoption.

## Research Questions

**RQ1.** To what extent do the dimensions of trust (security, privacy, and perceived risk) relate to the behavioral intentions to adopt FIM, in conjunction with by the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business?

**H1$_{0}$:** There is no correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**H1$_{a}$:** There is a correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**H1$_{01}$:** There is no correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{a1}$:** There is a correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{02}$:** There is no correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{a2}$:** There is a correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03}$:** There is no correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03a}$:** There is a correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

## Definition of Terms

**Adoption.** Rogers defined adoption in the diffusion of innovations theory "as a consumer's positive decision to accept and use an innovation, which ultimately leads to a positive investment decision and actual use" (as cited in Senk, 2013, p. 3).

**Behavioral intention.** Lai and Chen (2011) defined behavioral intention as the "likelihood to engage in a certain behavior are important indicators of customers' future behaviors" (p. 319). Behavioral intention and actual use are two variables in the unified theory of acceptance and use of technology.

**Effort expectancy.** Venkatesh et al. (2003) defined effort expectancy as individuals' perception of the level of difficulty or ease associated with the use of technology. Venkatesh et al. (2003) captured three constructs from the existing technology adoption models into this concept: perceived ease of use (technology acceptance model [TAM1]/TAM2), complexity (model of personal computer utilization [MPCU]), and ease of use (innovation diffusion theory [IDT]). Perceived ease of use refers to the effortlessness of using IT; complexity refers to the difficulty to use a system, and ease of use refers to using innovation or enhancement to make technology easy to use.

**Facilitating conditions.** Venkatesh et al. (2003) defined facilitating conditions as the degree to which an individual believes that resources and support exist to use IT. The concepts of facilitating conditions come from three different constructs and models (Venkatesh et al., 2003): perceived behavioral control (theory of planned behavior [TPB]/decomposed theory of planned behavior and C-TAM-TPB [combined TAM and TPB]), facilitating conditions (MPCU), and compatibility (IDT).

**Federated identity management (FIM).** FIM facilitates both flexible authentication methods and federated authorization management (Chadwick et al., 2014). Federated identity management is a technology that allows users to sign into multiple service providers using the same credentials. Federated identity management leverages SSO solutions, which are an emerging technology that has an aim of providing convenience and seamless access to information resources without using different login credentials to authenticate to each system.

**Perceived risk.** Zhou (2012) defined perceived risk as disclosure of personal information when using technology that causes users to be pessimistic about future impacts of such disclosure. Masoud, 2013 defined risk from the perspective of consumers as the uncertainty and adverse consequences of adopting a product or service. Uncertainty is the likelihood of unfavorable outcomes and consequences of the adverse event. Perceived risk is a significant influence in negatively affecting the adoption intentions of consumers (Claudy, Garcia, & O'Driscoll, 2015; Kleijnen, Lee, & Wetzels, 2009).

**Performance expectancy.** Venkatesh et al. (2003) described performance expectancy as the level at which using IT provides benefits to consumers by enhancing their job performance. It implies that people are more likely to adopt new technological solutions when they believe it will enhance their job performance. Venkatesh et al. captured five constructs from various technology adoption models that pertain to performance expectancy. For example, Venkatesh et al. captured perceived usefulness from TAM1/TAM2 and C-TAM-TPB, extrinsic motivation from the motivational model, job fit from the MPCU, relative advantage from IDT, and outcome expectations from social cognitive theory.

**Privacy.** Zhou (2012) defined privacy as a concern of individuals related to personal information disclosure resulting from the use of technology. According to Article 12 of the United Nations Declaration of Human Rights, privacy is a fundamental right that is crucial to autonomy and the protection of human dignity.

**Security.** Security is a process of maintaining the confidentiality, integrity, and availability of data.

**Single sign-on (SSO).** Single sign-on is an authentication service that allows end users to authenticate with one set of login credentials to access multiple applications or systems (Tmušić & Veinović, 2017).

**Social influence.** Venkatesh et al. (2003) defined social influence as the extent to which social pressure influences individual perceptions of a particular technology.

**Trust.** Lo (2010) defined trust as the beliefs that reflect the confidence of users that the personal information they submit will receive competent, benevolent, and honorable treatment.

## Research Design

This research study included a quantitative, nonexperimental survey to examine the effect of trust and the UTAUT model on the technology adoption using inferential statistical models to test hypotheses and answer the research question. The researcher employed a random sampling technique to gather data from various IT decision makers across the United States. Sampling demography was IT decision makers between the ages of 21 and 70. The researcher included a screening question at the beginning of the survey to screen out participants who had switched roles within an organization and were no longer qualified to participate. The researcher administered the survey instruments of Zhou (2012) and Opala (2012) to randomly selected participants.

The researcher used Qualtrics, a professionally administered survey system, for data collection; provided the survey instruments and sampling criteria to a Qualtrics account manager to randomly selected participants; and received 168 completed questionnaires. The researcher obtained informed consent from all the randomly selected participants before allowing access to the survey. Qualtrics sent and retrieved completed questionnaires. To protect the participant's privacy, the Qualtrics account manager anonymized the responses by removing all personally identifiable information before providing coded data to the researcher. The researcher stored the data set on a full-disk-encryption hard drive on a biometrically protected Surface Pro 4 laptop.

The researcher used multiple regression analysis to examine the correlation between trust (security, privacy, and perceived risk), the UTAUT constructs, and behavioral intention to adopt FIM. The researcher applied various statistical techniques and approached to report the data, analyze the data, answer the research question, and test the research hypotheses. The researcher used a regression analysis of latent variables based on the optimization technique of the partial least squares (PLS) to elaborate the model that represented the relationships between the predicted and observed variables (Hair, Sarstedt, Ringle, & Mena, 2012). PLS is a multivariate technique used to test structural models to find the fundamental relationship between two matrices (Hair et al., 2012). Researchers can use PLS for theory confirmation, as it can indicate where relationships might exist and reveal propositions for testing later (Chin, 1998). Partial least squares (PLS) compose of a structural part reflecting the relationships between latent variables and a measurement component (Escobar-Rodríguez & Carvajal-Trujillo, 2014).

Data analysis for this study involved a two-stage approach to establishing the data quality of the research model. The first stage was the development and evaluation of the measurement model, and the second stage involved the development of a full structural equation model. Structural equation modeling (SEM) provides flexibility to perform model relationships, construct unobserved latent variables, model errors, and statistically test a priori theoretical and measurement assumptions against empirical data (Chin, 1998).

## Assumptions and Limitations

### Assumptions

The attitude, personality, and value of the top management play a critical role in the organizational decision-making process. Several studies revealed that the top management's role in any organization is decisive, as their decisions may positively or negatively affect the current and future activities of the company (Amaio, 2009; Chaudhry, Chaudhry, & Reese, 2012; Shang & Lin, 2010). Many organizational leaders do not adopt FIM due to concerns about trust (i.e., security, privacy, and perceived risk) that may result from unauthorized access to their personal and their customers' data. This study included an assumption that IT decision makers orchestrate and support the failure to adopt FIM. The study also included an assumption that the organization structure is centralized (i.e., executives make all the organizational decisions without lower level personnel's input). As senior management plays a critical role in the decision-making process, successful adoption of innovative technology depends on its alignment with vision and organization's enterprise architecture, due consultation, visible support, and commitment from top management (Amaio, 2009; Shang & Lin, 2010). In alignment with the first assumption, the second assumption was that the decision not to adopt FIM occurs without outside or other influences.

### Limitations

A limitation of the study was that the focus was on FIM adoption at the organization level and sample size. Future research could involve studying adoption at the individual level and focusing on those who have adopted FIM. Voluntary studies can include potential biases, as participants may be unwilling or unable to participate in the survey (Fowler, 2009). Another limitation was that the study could have introduced a response bias. For example, the researcher might have twisted the questions in a way that unduly favored one response over another.

Although FIM can lead to economic benefits to organizations, the adoption of this technology has not been a factor in the perceived value of the technology. Another limitation was that security, privacy, and perceived risk could have a direct effect on predicting behavioral intentions to adopt FIM. Even though several researchers have conducted studies on UTAUT constructs, none of the researchers considered the direct effect of these constructs on the behavioral intention to adopt innovative technology.

## Organization of the Remainder of the Study

Chapter 2 contains a literature review of FIM and relevant topics on federated identity processes, technologies used, trust frameworks, and UTAUT model. Chapter 3 includes a discussion on the purpose of the study; the target population and sampling, including the power analysis to determine the sample size; the research design; and the research methodology used throughout the study. Chapter 4 presents the data analysis and the results obtained by conducting various types of statistical analyses appropriate for this study based on the research question and hypotheses derived from the research problem and purpose. Chapter 5 concludes with the results, implications, synthesis, and evaluation of data analysis and recommendations for further research.

# CHAPTER 2. LITERATURE REVIEW

## Methods of Searching

This quantitative correlation study involved investigating, analyzing the result, and identifying the meaningful relationship between the dimensions of trust (security, privacy, and perceived risk), UTAUT model constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intention to adopt FIM in U.S. business settings. The researcher conducted a comprehensive review of relevant literature to outline the intellectual progress of research in FIM adoption. The literature review begins with a search of databases available at the Capella University Library, such as Business Source Complete, Computers & Applied Sciences Complete, Computing Database, Credo reference, ACM Digital Library, Academic Search Premier, Summon, Dissertations and Theses Global, and Google Scholar. The study involved using various search techniques to find relevant references using the following keywords or combinations of keywords to retrieve the most significant articles: federated identity, UTAUT, TAM, technology adoption, trust, security, privacy, and perceived risk. The researcher also leveraged RefWorks, a reference management tool, to ensure a more efficient and reliable process for gathering, to organize, reading, and to cite research materials.

The researcher synthesized scholarly and peer-reviewed articles related to various models of technology adoption and emphasized the UTAUT as the model that support FIM adoption. The researcher also discussed the background and history of FIM, FIM systems, technologies used in FIM, and factors influencing FIM adoption. Lastly, the researcher discussed the limitations of UTAUT. Figure 2 is a visual representation of the review of the relevant literature.

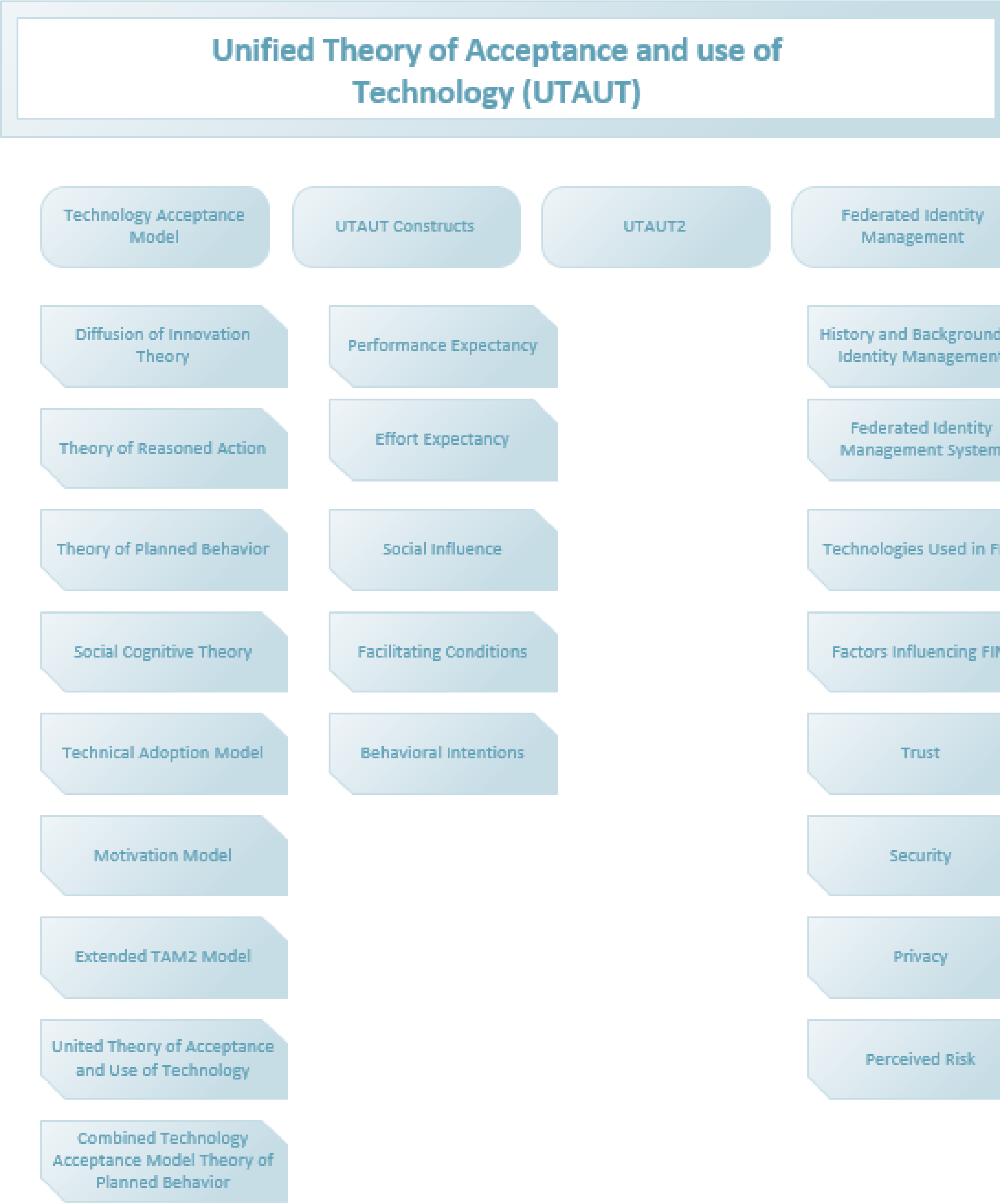

Unified Theory of Acceptance and use of Technology (UTAUT)
Technology Acceptance Model
UTAUT Constructs
UTAUT2
Federated Identity Management
Diffusion of Innovation Theory
Performance Expectancy
History and Background Identity Managemen
Theory of Reasoned Action
Effort Expectancy
Federated Identity Management System
Theory of Planned Behavior
Social Influence
Technologies Used in F
Social Cognitive Theory
Facilitating Conditions
Factors Influencing FI
Technical Adoption Model
Behavioral Intentions
Trust
Motivation Model
Security
Extended TAM2 Model
Privacy
United Theory of Acceptance and Use of Technology
Perceived Risk
Combined Technology Acceptance Model Theory of Planned Behavior

*Figure 2.* Visual representation of literature review

## Theoretical Orientation for the Study

The theoretical framework that guided this research was the original UTAUT conceptual framework developed by Venkatesh et al. (2003). Venkatesh et al. developed the model by conducting a review of and comparing, eight prominent models of technology adoption to formulate a unified model that integrated elements across each model. The original theory included four primary constructs or independent variables, which were performance expectancy, effort expectancy, social influence, and facilitating conditions, and two dependent variables, which were the behavioral- intention and the use behavior. The model also included moderating variables: age, gender, experience, and voluntariness of using innovative technology in the workplace (Venkatesh et al., 2003). Venkatesh et al. based the UTAUT model on user acceptance of IT with the goal of explaining user intentions to adopt a technology and subsequent usage behavior.

Since its formation, various theorists have used UTAUT as a yardstick for explaining and predicting the adoption of various technologies in both organizational and non-organizational settings (Lee et al., 2010; Tan, 2013; Venkatesh et al., 2012). Several applications and replications of the theory or part of the theory in organizations "have contributed to fortifying its generalizability" (Venkatesh et al., 2012, p. 158). Many technology adoption researchers have employed UTAUT2 to translate the UTAUT model to the consumer context (Lee et al., 2010; Odeyinde, 2014; Slade, Williams, & Dwivedi, 2014; Tan, 2013; Venkatesh et al., 2012). This study extends the practicality of the UTAUT2 model in FIM, which was a task Venkatesh et al. (2003) did not consider. Figure 3 is a conceptual model adapted from Venkatesh et al. (2003).

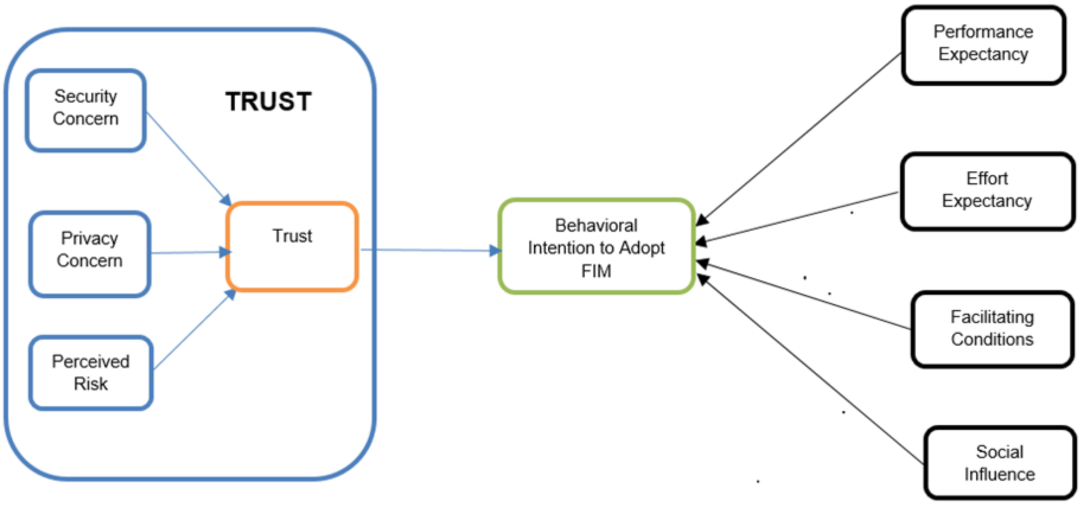


*Figure 3.* The conceptual model of user acceptance of federated identity management

## Review of the Literature

### Theory of Reasoned Action

Ajzen and Fishbein (1969) formulated TRA and further revised and expanded it in the 1970s. Theory of reason action was one of the first and most widely used social-psychological models for predicting human behavior based on preexisting attitudes and behavioral intentions (Ajzen & Fishbein, 1980). Theory of reason action is one of the three persuasion models (Southey, 2011). Fishbein and Ajzen developed the model with the aim of explaining the relationship between attitudes and behaviors within human action. Ajzen (1985) introduced TRB as an extension of TRA by incorporating perceived behavior intentions as an antecedent to behavioral intention. Ajzen (1991) later extended the TRA boundary condition by adding non volitional control (i.e., making a conscious decision).

Several theorists have applied the TRA model to communication (i.e., college fraternity and sorority hazing), knowledge sharing in companies, customer behavior (e.g., coupon usage and brand loyalty), and sexual behavior (i.e., condom use and sexual behavior in teenage girls). For example, Dippel, Hanson, McMahon, Griese, and Kenyon (2017) applied the theory to predict green product consumption. Dahl, Tagler, and Hohman (2017) used the theory to predict future gambling behavior. Tagler, Stanko, and Forbey (2017) applied the theory to predict sleep hygiene, and Ha and Janda (2017) applied the model to predict consumer intentions to purchase energy-efficient products. Figure 4 is a theory of reasoned action conceptual model.

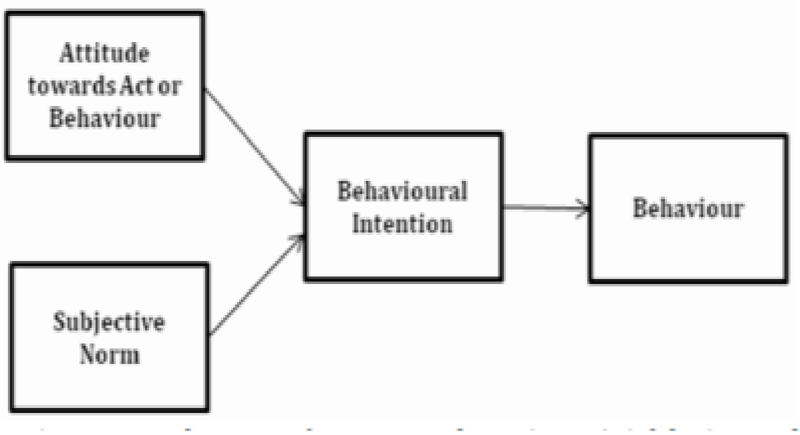


*Figure 4.* Theory of reasoned action. Reprinted from “The Prediction of Behavioral Intentions in a Choice Situation,” by I. Ajzen and M. Fishbein, 1969, *Journal of Experimental Social Psychology*, *5(4)*, p. 400–416. Copyright 1969 by Elsevier Inc. Used with permission

.

Despite the popularity of TRA, many researchers have criticized the model as not taking into consideration personality and demographic variables. The model also led to much ambiguity concerning perceived behavioral control and thereby created measurement problems. Many researchers believed an anchor of the model was that people are rational and make systematic decisions based on available information. The model did not include a way to consider unconscious motives.

### Theory of Planned Behavior

Ajzen (1985) developed and introduced TPB as an extension of TRA by incorporating an additional variable to determine intention and behavior. The theory was developed as an improvement to the predictive power of the TRA and perceived behavioral control (i.e., predicting deliberate human behavior, since human behavior can either be deliberative or planned). The theory included an assumption that behavioral intention has a direct influence on individual's behavior and that perceived behavioral control and attitudes, subjective norms, and perceived behavioral control shaped behavioral intentions (Ajzen, 2011; Fogarty & Shaw, 2010). The theory serves to link belief and behavior. Self-efficacy is one of the most consistent predictors of both the adoption and maintenance of physical activity (Bauman et al., 2012). According to Ajzen (2011), three types of consideration guide human action, and these considerations are crucial mainly when changing human behavior. The considerations are behavioral beliefs, normative beliefs, and control beliefs. Behavioral beliefs refer to beliefs about the expected result or consequences of the behavior (Ajzen, 2011). Normative beliefs are a belief in the normative expectations of others (Ajzen, 2011). While control beliefs are a belief in the presence of factors that may expedite the performance of people (Ajzen, 2011). One of the biggest criticisms is that the model has limited explanatory power. Figure 5 is a theory of planned behavior conceptual model.

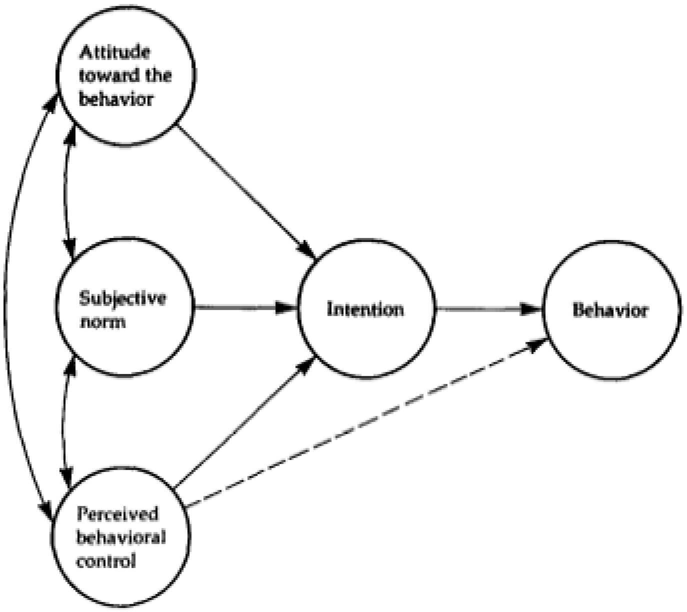


*Figure 5.* Theory of planned behavior. Reprinted from “The Theory of Planned Behavior” by I. Ajzen, 1991. *Organizational Behavior and Human Decision Processes 50(2),* p.182. Copyright 1991 by the Academic Press, Inc. Used with permission.

**Technology Acceptance Model**

The TAM is an IT model initially proposed by Davis (1985) as an instrument for predicting IT usage. Davis built the model on TRA and grounded it on the premise that attitude, beliefs, and intentions can describe technology acceptance and use (Turner, Kitchenham, Brereton, Charters, & Budgen, 2010). The original model measured actual usage of four internal variables: perceived ease of use, perceived usefulness, attitude toward use, and behavioral intention to use (Davis, 1985). Venkatesh and Davis (2000) later proposed a second version of the TAM (TAM2) as a modification to the original TAM, because the previous model did not incorporate attitude toward use. The new theory incorporated two additional variables: experience and subjective norm.

Since inception, various organizational leaders and users have applied TAM and TAM2 to a variety of technology products and services as a mechanism for predicting the likelihood of users' intention. For example, Holden and Karsh (2010) applied the theory to health IT, and Y. H. Lee, Hsieh, and Hsu (2011) applied the theory to an e-learning system. Shroff, Deneen, and Ng (2011) applied the theory to an e-portfolio system; Chung, Park, Wang, Fulk, and McLaughlin (2010) applied it to online community participation, and Kesharwani and Singh Bisht (2012) applied it to Internet banking. Figure 6 is a conceptual model of technology acceptance model.

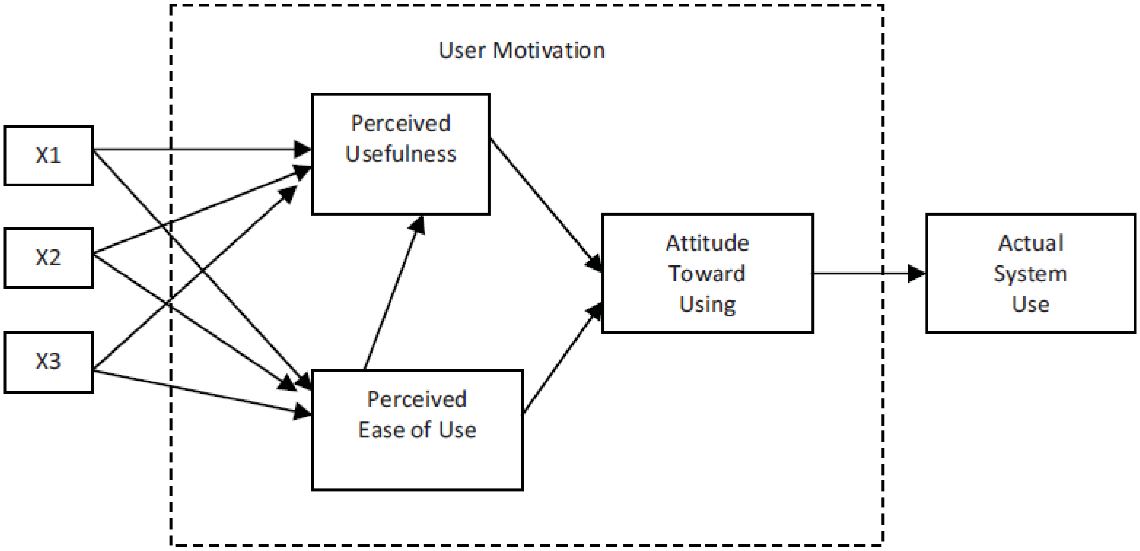


*Figure 6*. Original technology acceptance model. Reprinted from "A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results" by F. D. Davis, 1985, *Doctoral dissertation, Massachusetts Institute of Technology*, p. 24. Copyright 1985 by the Massachusetts Institute of Technology. Used with permission.

Though researchers use TAM quite frequently, numerous researchers have shared their apprehension regarding its philosophical accuracy and practical usefulness (Benbasat & Barki, 2007; Chuttur, 2009). Chuttur (2009) noted that TAM's testing methodology included bias, the poor philosophical relationship among the constructs was old, and the model had limited explanatory and predictive power. According to Bagozzi (2007), TAM is highly generalized and attempting to acclimate the model to continually changing IT environments will lead to theoretical chaos and confusion. Benbasat and Barki (2007) also noted that the model seems to distract scholars from examining and comprehending the issue, and the theory also pretended to advance the scientific knowledge base.

### Technology-Organization-Environment

Tornatzky and Fleischer (1990) developed the technology-organization-environment (TOE) theory, and it is one of the best-supported theories and models recommended for technology acceptance. Technology-organization-environment is an organization-level theory that depicts how technology, organization, and the environment can influence the process of adopting and implementing a technological innovation (Al-Mamary, Al-nashmi, Hassan, & Shamsuddin, 2016; Baker, 2012). The model identifies three facets of an organization's context that influence technology adoption and implements technological innovation, which is technological, organizational, and environmental contexts. Each context presents challenges and opportunities for adopting innovative technology. The TOE theory has garnered extensive empirical support from many technology adoption researchers. For example, Cao, Jones, and Sheng (2014) applied the TOE framework to gain insights regarding contextual influences on the adoption of patient-tracking radio-frequency identification (RFID), including some RFID-specific issues. Based on the TOE framework, Wang, Li, Li, and Zhang (2016) explored why hotel leaders adopt mobile reservation systems. The study provided several theoretical and practical implications related to mobile service adoption. Awa, Ukoha, and Emecheta (2016) used the TOE theoretical framework to study the adoption of enterprise resource planning solutions. Researchers who apply the framework provide further insight into information system adoption by investigating how 12 factors within the TOE framework explain how IT executives adopt enterprise resource planning solutions.

## Technological Context

The technological context includes the characteristics and the usefulness of the innovative technology. The technological context refers to both internal technologies such as management, employees, products, and services and external technologies relevant to an organization. The technological context is an essential component of the TOE that affects the adoption process (Oliveira & Martins, 2011). Kuan and Chau (2001) corroborated the notion of the significance of technology resources in terms of the level of IT sophistications and management as a major factor that influences a successful information technology adoption. The study of Zhu, Kraemer, Xu, and Dedrick (2004) emphasized the importance of technology as a driver for e-business, the organization can make efficient use of Internet technologies and exhibit technology readiness to create e-business value. Moreover, sufficient financial resources help the organization to acquire the necessary information technology resources and achieve successful e-business implementation (Wen & Chen, 2010; Zhu et al., 2004).

## Organizational Context

The organizational context is descriptive and directly relates to the availability and use of internal resources such as organizational structure, communication processes, size of the organization, human resources quality, amount of slack resource and linkages among employees (Baker, 2012; Oliveira & Martins, 2011). The organizational context also represents an existing relationship among distinct roles within an organization. Organizational structure is one of the most commonly studied organizational aspects in the innovation or information technology adoption literature and it specifies how business activities are allocated, coordinated and supervision are directed toward the achievement of organizational business purposes (Ahmadi, Nilashi, & Ibrahim, 2015; Palacios-Marqués, Soto-Acosta, & Merigó, 2015; Wang et al., 2016). Organization structure also determines how information flows between levels within an organization (Wang et al., 2016). Various studies on individual-level behavior have found support for the significant impact of subjective norms on information technology initial adoption (Venkatesh et al., 2012).

**Environmental context**

The environmental context refers to an environment where organizational leaders conduct business. The environmental context consists of numerous stakeholders such as industry members, competitors, suppliers, customers, regulatory influence, industry pressures, the government, vendor influence, and the community (Angeles, 2014). The stakeholders can influence the organizational ability to interpret and acquire resources to pursue technology innovation (Angeles, 2014). Figure 7 is a conceptual model of the TOE.

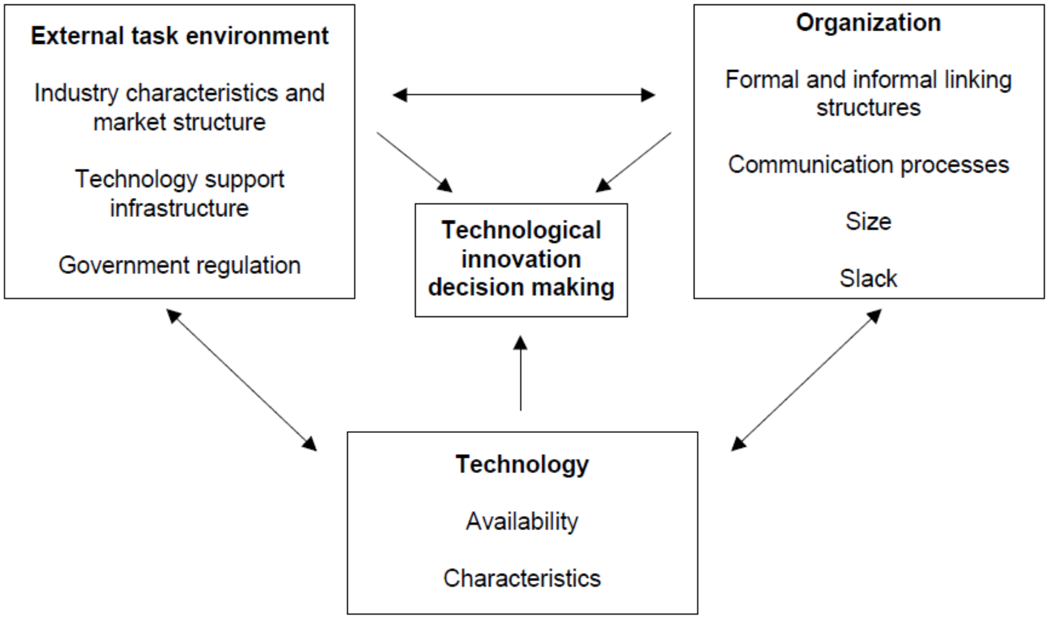

External task environment
Industry characteristics and market structure
Technology support infrastructure
Government regulation
Organization
Formal and informal linking structures
Communication processes
Size
Slack
Technological innovation decision making
Technology
Availability
Characteristics

*Figure 7*. Technology, organization and environment framework. Reprinted from “The Role of Market Research in the Development of Discontinuous New Products,” by P. Trott, 2001, *European Journal of Innovation Management, 4(3)*, p. 117-125. Copyright 2001 by the Emerald Publishing Limited. Used with permission.

Senior executives can play a significant role in the technology acceptance process, and they must have at least some level of background in IT, change management, environmental knowledge, and future IT trends (Tran, Zhang, Sun, & Huang, 2014). Vijay, Durbhakula, and Kim (2011) contended that some researchers had viewed the framework from the organization-level perspective, which led to an inadequate exploration of the contexts at the multinational level. Baker (2012) noted that the focus of most previous studies was on individual organizations and suggested conducting research on the choices available to a group or a conglomerate of companies whose leaders decide to adopt innovative technology and whether leaders of dominant firms within the value chain believe in the adoption of innovative technology more than in the value chain partners.

## Unified Theory of Acceptance and Use of Technology

The UTAUT is a technology acceptance theory developed by Venkatesh and others to explain IT acceptance and use (Venkatesh et al., 2003). Many technology adoption researchers have used the most popular models presented to explain and predict user acceptance of IT (Lee et al., 2010; Odeyinde, 2014; Slade et al., 2014). The foundation of the UTAUT model is the TAM and the TPB. Venkatesh et al. identified four critical constructs in the original theory. These independent variables or constructs are performance expectancy, effort expectancy, social influence and facilitating conditions and they influenced the dependent variables of behavioral intention and usage (Venkatesh et al., 2003). The model also included moderating variables: age, gender, experience, and voluntariness of using innovative technology in the workplace (Venkatesh et al., 2003). Figure 8 shows the original UTAUT conceptual model.

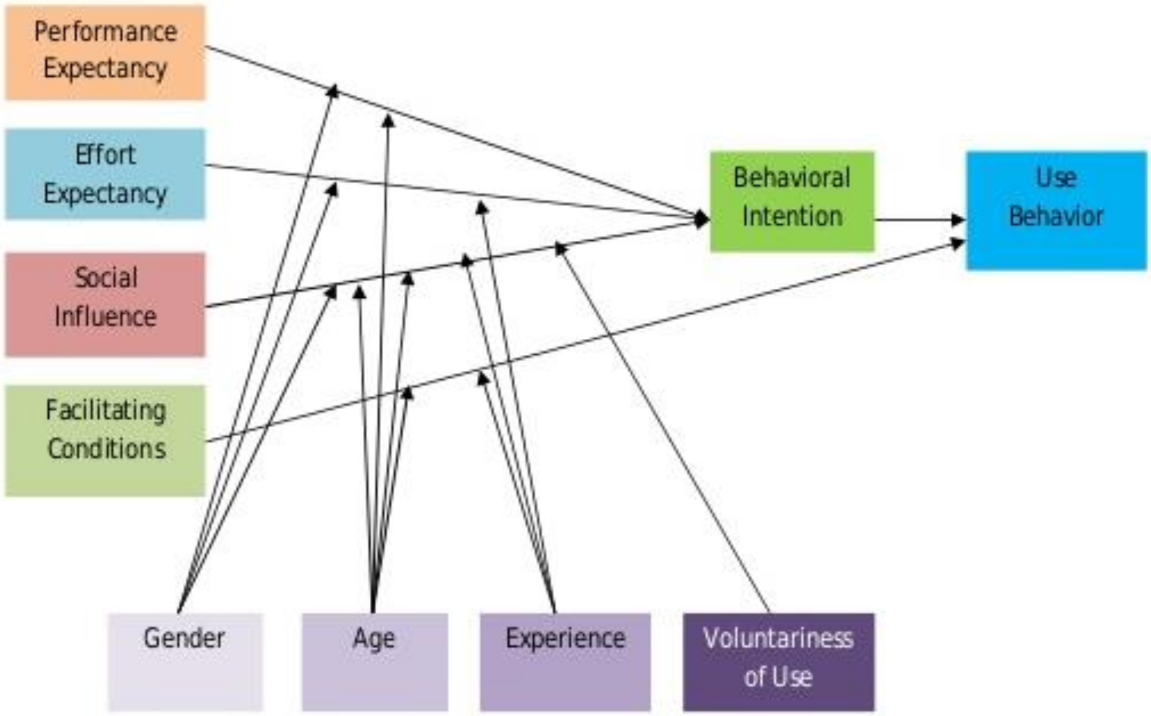


*Figure 8*. Original unified theory of acceptance and use of technology model. Reprinted from "User Acceptance of Information Technology: Toward a Unified View" by V. Venkatesh, M. G. Morris, G. B. Davis and F. D Davis, 2003, *MIS Quarterly*, *27(3)*, p. 447. Copyright 2003 by the Regents of the University of Minnesota. Used with permission.

Some IT adoption researchers primarily used the theories in psychology, sociology, and information systems to explain individuals' intention to adopt innovative technologies (Corazao, 2014; Tate, Evermann, & Gable, 2015; Venkatesh et al., 2003). Researchers frequently use the UTAUT in their studies to explain and predict user acceptance of IT (Lee et al., 2010; Slade et al., 2014; Venkatesh, Davis, & Morris, 2007). Since its development, several technology researchers have extended the theoretical boundaries of UTAUT to expand the understanding of technology adoption. For example, Venkatesh et al. (2012) extended the UTAUT to investigate the adoption and use of IT in a consumer context. Venkatesh et al. (2012) proposed UTAUT2 and incorporated hedonic motivation, price value, and habit into the original constructs of UTAUT. Vedenhaupt (2016) applied the UTAUT framework to analyze and identify relationships between social media use by arts audiences and ticket sales at small nonprofit performing arts organizations. Tan (2013) also applied the UTAUT model to understand factors affecting the use of English e-learning websites in Taiwan. Using the UTAUT framework, Pope (2014) explored the variables that affect individuals' intention to use business intelligence technology in organizations.

Though UTAUT appeared to be ideal for studying technology innovation adoption due to its applicability to the topic, the model still faces some level of criticism from innovation adoption researchers. Im et al. (2008) noted that the original model did not include trust. Lee et al. (2010) also revealed the critical role trust plays in users' acceptance of IT. The study of Venkatesh et al. (2008) revealed that behavioral intention does not appear as an external factor that can influence the performance of behavior. Venkatesh et al. (2008) study also revealed that behavioral intention has a weak predictive and explanatory ability to address uncertainty and unforeseen circumstance between and after the intention is formed and performed and also, cannot predict behaviors that are not totally within an individual's discretionary control. Technology adoption researchers have applied the UTAUT to technology adoption at the firm level, but the model was not suitable for studying individual perspectives of behavioral intention towards adopting and using an information system (Moghavvemi, Salleh, & Abessi, 2013). Venkatesh et al. (2003) did not address attitude and self-efficacy which are a direct determinant of behavioral intention in the original model. Further research has demonstrated that perceived overall self-efficacy contributes somewhat to the encouragement and fulfillment of individuals (Straub, 2009; Venkatesh et al., 2003).

## Identity Management

International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 4760-1 defines identity as a "set of attributes related to an entity." Even though various researchers have used the concept of identity in a different context but there has not been a single definition (Perry & Pollock, 2016). Identity is a peculiar character or personality of an individual that consists of traits, attributes of an identifier such as, password, social security number or user profile, and preferences upon which one may receive personalized services (Cao & Yang, 2010). In this study, identity is described as the representation, proofs, and credentials of the subject used in accessing information technology resources of an organization. It is the process of identifying, authenticating and authorizing users to an organization’s information resources. Identity management involves issuing digital identities and credentials for authentication and combines with the subscriber proven identity with their authorization. The goal is to ensure that the identity provider grant access to only authenticated users to the specific information system resources. Identity management system (IdM) according to Perera (2017) is the security and business processes, policies and technologies that “enables the right individuals to access the right resources at the right times and for the right reasons” (p.1). It is the mechanism used in the information system to control identity. Identity management system is a tool for managing identities in today’s digital world.

### Common Identity Management Systems Model

***Centralized identity management.*** In this model, the service provider entrusts identity providers with identity linking, i.e., each service provider uses the same identifier and credential (Birrell & Schneider, 2013). This model permits a dedicated identity provider to manage all user’s identities and separate functions of the service provider and the identity provider. The subscriber must trust the identity provider by disclosing all user attributes, even, when the subscriber chooses to create multiple distinct identities (Birrell & Schneider, 2013). Since the service provider store user’s identities in the same identity provider, the subscriber’s pattern attribute could be easily linked to the same individual. Example of a centralized identity management model is public key infrastructure (PKI), where a trusted party called Certificate Authority (CA) issues certificates to entities and individuals after verifying their identity. The subscribers can then use the same certificate to gain access to different services. Other examples of a centralized identity management model are Facebook Single sign-on (SSO), Kerberos Authentication Server and Microsoft Network Passport. The major drawback is that it can create a potential single point of failure should one of the trusted identity providers fail and thereby could affect the business operation of the service providers (Birrell & Schneider, 2013; Cusack & Ghazizadeh, 2016; Olden, Platt, Royer, Berg, & Wallingford, 2015).

***Decentralized identity management.*** In this model, each user is required to have an identifier for each service. This model does not allow identity linking, i.e., the identity provider can only trust the attributes the service provider release to them (Birrell & Schneider, 2013). In the decentralized model, the service provider plays both the service and the identity provider’s role. In today’s digital world, this model is common in most transaction due to its relatively simple to manage. However, this model is rapidly becoming too challenging to manage for users (Bonneau et al., 2015).

***Federated identity management***. Federated identity management is a solution that simplifies the account management problem and provides economic advantages and convenience to the organizations and their subscribers (Ayed, & Ghernaouti-Hélie, 2012; Chadwick et al., 2014; Kurowski, 2015). Federated identity solutions allow a given credential service provider to provide authentication and (optionally) subscriber attributes to a numerous separately administered on relying parties (Grassi, Garcia, & Fenton, 2017).

**Federated Identity Management**

Since the advent of IT, the use of passwords in protecting information systems from unauthorized access has dominated the computer authentication process, despite increasing interest among industry leaders, academia, and researchers in substituting this technology with a more robust, secure, and user-friendly technology (Bonneau et al., 2015). Bonneau et al. (2015) considered passwords to be a string of characters used to validate a user's identity during the authentication process. It is one of the most common techniques used for securing critical and sensitive information.

The use of IT, particularly mobile technologies, continues to surge. According to a study conducted by researchers at the Pew Research Center in 2015, 68% of American adult owned a smartphone, compared to 35% in 2011, and mobile computer ownership had increased 45% among adults (Anderson, 2015). Most users use these devices to access their financial information online and do not know the extent of their risk exposure. Many organizational leaders are adopting mobile technology to access sensitive corporate information through the bring-your-own-device (BYOD) concept (Armando, Costa, Verderame, & Merlo, 2014). BYOD is the increasing trend of using employee-owned devices such as smartphones, laptops, or tablets to access organization resources. Users sometimes receive long and complicated login credentials to access various organizational information systems. The complexity of the passwords as prescribed in organization policy posed a significant burden on the users and security challenges to the organization, as the users could write down the password on a piece of paper. Hence, organizational leaders are continually trying to balance user convenience with security. The burgeoning in identity theft due to the misuse of global but unprotected identifiers like a credit card is also one of the reasons for the emergence of FIM.

The major identity crisis the world faced today was as a result of a vast majority of identity and authentication processes are performed on the internet between the service provider and their customers (Schweighofer, E., & Hötzendorfer, 2013). Another issue was that individual service providers collect more information on individual users which generate privacy concerns Schweighofer, E., & Hötzendorfer, 2013). Addressing the security and privacy challenges of the traditional password with a modern approach led to the formation of FIM. Federated identity management is an emerging technology in which subscribers of multiple enterprises and business partners use a standard login and authentication process to gain access to the entire networks, services and applications (Jensen, 2011; Temoshok & Abruzzi, 2016). Federated identity management involves the creation of global interoperable identities such that organization can have a common identity federation to share authentication processes and access multiple resources and services (Haghshenas & Seyyedi, 2012; Temoshok & Abruzzi, 2016). Several initiatives and systems have utilized the FIM concept such as Microsoft Passport, OpenID and Liberty Alliance Project, Facebook, and Google to access different services or online resources.

Many researchers have shown that FIM offers an economic advantage such as cost reduction in managing individual identities, as well as efficient and convenient ways of delivering identity services between different organizations (Arias-Cabarcos et al., 2012;

Catuogno & Galdi, 2014; Lynch, 2011). Jensen (2011) contended that no researchers had presented the real savings of FIM. An organizational leader can also proactively recognize and manage risk across multiple enterprises. Other benefits are rapid online service provisioning, increased customer base, and increased ease of access to shared services (Temoshok & Abruzzi, 2016). Catuogno and Galdi (2014) revealed that FIM is a crucial concept for identity management that offers continuous access to technologies and services. It is an impetus to integrating IT services and solutions that bridge various trust domains to allow the exchange of identity information to improve usability (Arias-Cabarcos et al., 2012; Cabarcos, Almenárez, Mármol, & Marín, 2014). The study of FIM will sustain a steady growth as more technology and services such as mobile access, Internet of Things, and cloud technology will substantially gain support and integrate with the FIM (Lynch, 2011).

Establishing trust between identity providers is a critical component of identity federation. Trust enables subscribers to believe the statements made by a federation. Trust is the main reason consumers' attitude toward adopting FIM has not been favorable (AlQatan et al., 2012), even though FIM enables subscribers to mutually exchange identity information, irrespective of whether the subscribers have prior knowledge of each member's identity information.

## Federated Identity Management System

The three actors involved in FIM participation are users, identity providers and service providers (Bertino & Takahashi, 2010; Catuogno & Galdi, 2014; Maler & Reed, 2008).

***Users.*** Users are the subject of identity information and, in most cases, are the principal source of information. Users are entities or actors who require access to organization services or resources through interactions with applications and online services. Users perform this interaction through a user agent such as a browser or other software applications that communicate with a remote system on behalf of the subscriber (Hackett & Hawkey, 2012).

***Identity providers.*** Another name for identity providers is identity assertion providers. An identity provider is a website or service whose role is to verify or provide information to aid in validating the identity of a subscriber. An identity provider is an entity that has the responsibility of verifying or providing information to aid in validating the identity of subscribers, conducting an authentication management, and propagating data to the service provider (Bodnar, Westphall, Werner, & Westphall, 2016; Catuogno & Galdi, 2014; Hackett & Hawkey, 2012).

***Service provider*.** A service provider is responsible for storing, managing, and maintaining a set of user identities. The service provider delegates the authentication management process to IdPs [identity providers] and also performs authorization process using the disseminated set of attributes from the IdP (Bodnar et al., 2016; Catuogno & Galdi, 2014. Service providers are responsible for making authorization decisions through the accompanying authentication assertions. At times, the service provider or relying party may rely on a third party or external authentication service provider for identity authentication. Figure 9 shows the communication between the subscriber, IdP, and the RP.

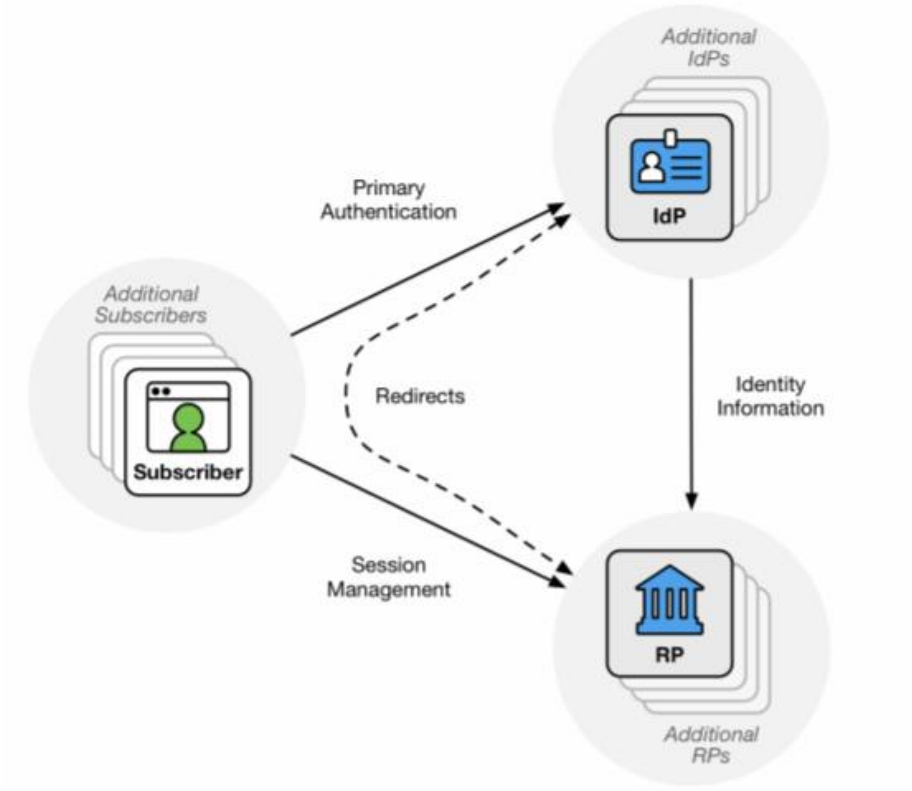


*Figure 9.* Federation identity management system. Reprinted from Digital Identity Guidelines: Federation and Assertions (No. Special Publication NIST SP 800-63C) (p. 8), by P. A. Grassi, E. M. Nadeau, J. P. Richer, S. K. Squire, J. L. Fenton, N. B. Lefkovitz, ... and K. Greene, 2017, by the National Institute of Standards and Technology

## How Does Identity Federation Management Work?

The process of federated identity starts from the creation of a federation between organization and business partners. When a subscriber visits the site of the organization that has an account in the federated member, the organization gives that subscriber a choice to federate her identity between the two organizations or to create a new account. If the subscriber approves, each organization generates a pseudonym and associates it with the individual's account at that organization. Then, the two organizations exchange the pseudonyms with each other. The next time such subscriber revisits any of the two organizations, she only needs to authenticate to one of them to use the services of both. As shown in Figure 10 the following steps adapted from Sun Microsystems (2010) shows a typical scenario of the federated identity management process:

1. Through the browser, the user accesses the service hosted by the service provider. The service provider creates a Security Assertion Markup Language (SAML) <AuthRequest>.

2. The service provider sends <AuthnRequest> to identity provider proxy for authentication.

3. The identity provider proxy redirects to identity provider discovery service.

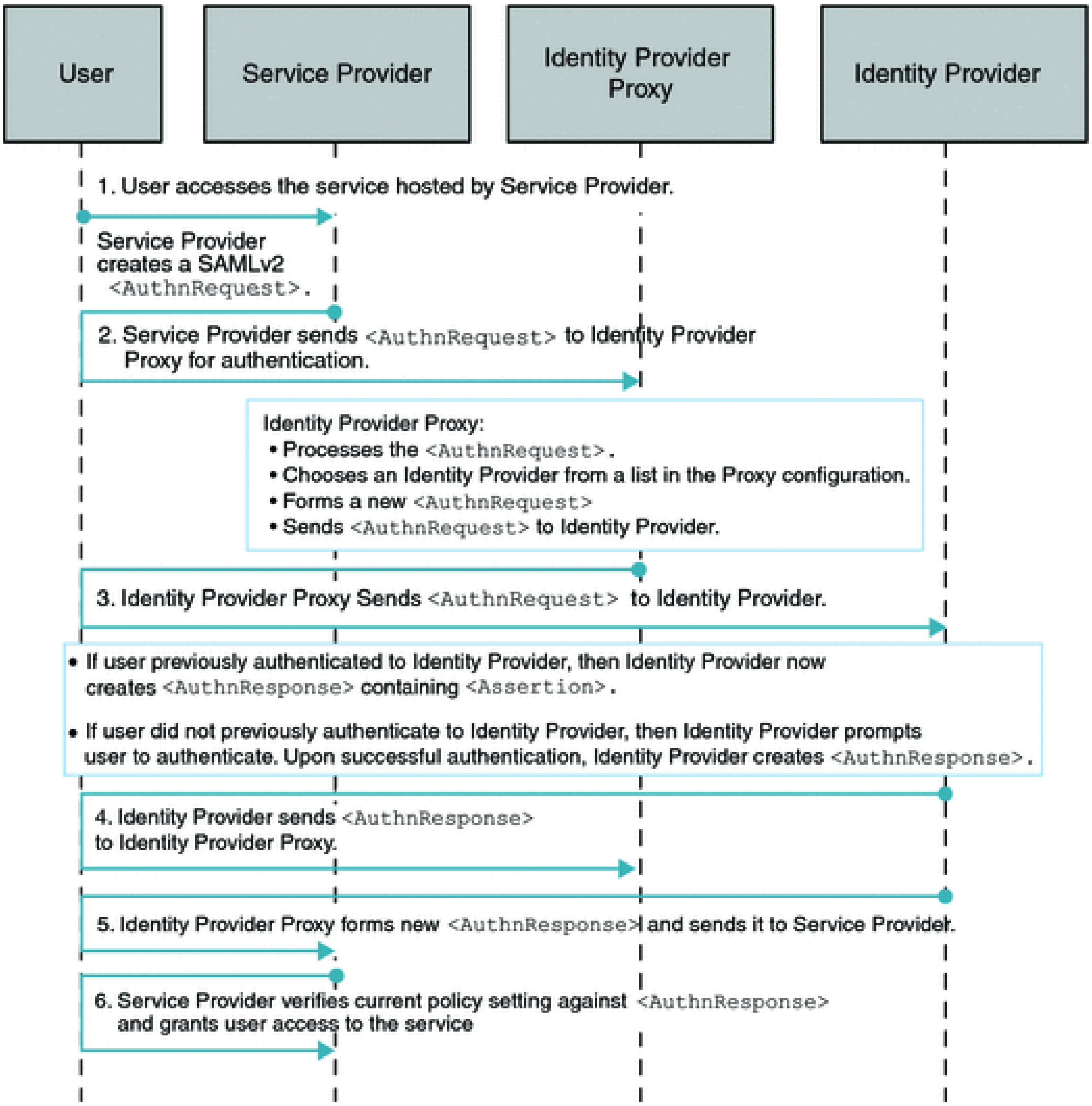
4. Identity provider discovery service returns the name of the preferred identity provider.

5. Identity provider proxy forms new <AuthnResponse> and sends it to the identity provider. If the user previously authenticated to the identity provider, then identity provider creates <AuthnResponse> containing <Assertion>, then identity provider prompts the user to authenticate upon successful authentication and identity provider creates <AuthnResponse>.

6. Identity provider sends <AuthnResponse> to identity provider proxy.

7. Identity provider proxy forms new <AuthnResponse> and sends it to the service provider.

8. Service provider verifies the current policy setting against the <AuthnResponse> information and grants the user agent access to the service.



1. User accesses the service hosted by Service Provider.

Service Provider creates a SAMLv2 <AuthnRequest>.

2. Service Provider sends <AuthnRequest> to Identity Provider Proxy for authentication.

Identity Provider Proxy:
- Processes the <AuthnRequest>.
- Chooses an Identity Provider from a list in the Proxy configuration.
- Forms a new <AuthnRequest>
- Sends <AuthnRequest> to Identity Provider.

3. Identity Provider Proxy Sends <AuthnRequest> to Identity Provider.

- If user previously authenticated to Identity Provider, then Identity Provider now creates <AuthnResponse> containing <Assertion>.
- If user did not previously authenticate to Identity Provider, then Identity Provider prompts user to authenticate. Upon successful authentication, Identity Provider creates <AuthnResponse>.

4. Identity Provider sends <AuthnResponse> to Identity Provider Proxy.

5. Identity Provider Proxy forms new <AuthnResponse> and sends it to Service Provider.

6. Service Provider verifies current policy setting against <AuthnResponse> and grants user access to the service

*Figure 10.* Illustration of Oracle identity federation with request and response process that can establish SSO authentication methodology. Reprinted from Implementing a SAMLv2 Identity Provider ProxySun, OpenSSO Enterprise 8.0 Deployment Planning Guide Implementing, by Sun Microsystems, Inc. 4150 Network Circle Santa Clara, CA 95054 U.S.A. Copyright 2010 by the Sun Microsystems, Inc. Used with Permission.

## Federated Identity Protocols

The most widely used federated protocols are SAML, Open Authentication (OAuth), OpenID Connect, Facebook Connect, and Google Friend Connect.

***SAML.*** The Organization for the Advancement of Structured Information Standards (OASIS) Security Service Technical Committee developed SAML in 2000. Many organizational leaders adopted the protocol as an open standard Extensible Markup Language (XML)-based framework for making security statements about subjects or sharing authentication and authorization between an identity provider and a service provider (Tschofenig et al., 2006). SAML2.0 is an enhancement to the original version that includes the Identity Federation Framework as specified by the Liberty Alliance Project. Many organizational leaders and academia have extensively used SAML2.0 in various Internet and intranet services. SAML specifies three components: assertions, protocol, and binding. The assertion is a security token in web service security. The protocols request and receive assertions, while binding defines the mapping of SAML request-response message exchanges to a Simple Object Access Protocol (Kim, 2009).

***OAuth.*** OAuth is an industry-standard protocol for authorization that provides a mechanism for users to access organization resources. OAuth allows the use of end users' account information by third-party services such as Twitter, PayPal, LinkedIn, and Facebook without exposing users' credential information. Due to the generalization of the protocol, distinct variations may not be compatible (Isaakidis, Halpin, & Danezis, 2016). Halpin and Cook (2012) interpreted OAuth as an authorization capabilities-based system, where the authorized access token can efficiently act as a capability to access attributes. The Internet Engineering Task Force's OAuth Working Group first proposed OAuth 1.0 protocol in 2006 and developed OAuth 2.0 in 2012. The OAuth 2.0 has become a de-facto standard for OpenID Connect (Fett, Küsters, & Schmitz, 2017). Researchers discovered numerous security flaws in OAuth 2.0. For example, Fett, Küsters, and Schmitz (2017) noted that the fundamental problem in OAuth was that identity providers blindly trust each other by logging every user transactions with a relying party and probably impersonate the user at the relying party and access their data. One of the significant drawbacks of OAuth 2.0 was that the framework enabled relying parties to obtain profile information about end users (Hardt, 2012; Li & Mitchell, 2016).

***OpenID Connect.*** OpenID Connect is an identity layer that sits above the OAuth protocol (Sakimura, Bradley, Jones, de Medeiros, & Mortimore, 2014). This protocol permits verification of the identity of an end user by computing clients based on the authentication performed by an authorization server and allows the retrieval of personal data given as key-value pairs such as proof-of-authentication, name, age, and photos (Sakimura et al., 2014). The protocol allows a variety of clients to transmit and receive data about authenticated sessions and the end users. The OpenID Connect requires interactions between 4 different parties: end user, user agent, OpenID provider, and relying party.

***Facebook Connect.*** In 2008, Facebook developed Facebook Connect as an SSO solutions/authentication protocol that allows users to interact with other websites through their Facebook account. It is a component of Facebook's Open Graph application programming interface (API) that permits third-party sites to integrate with Facebook to communicate bidirectionally to create an engaging and more vibrant social experience on the Internet (Ko, Cheek, Shehab, & Sandhu, 2010).

***Google Friend Connect.*** Google Friend Connect, developed in 2008, is a decentralized approach that allows users to use a credential issued by an OpenID identity provider to authenticate and share a profile, social-graph, and content data through third-party sites. Like

Facebook Connect, Google Friend Connect leverages open standards such as OpenID, OAuth, and OpenSocial with the aim of preventing users from having to register for the additional credential (Ko et al., 2010).

## Prior Findings

The review of previous studies revealed common approaches, patterns, and themes across studies that led to the attempt in the current study to understand the relationships between trust (security, privacy, and perceived risk perceptions) and FIM adoption. Synthesizing the literature revealed some of the trust factors influencing FIM.

## Trust

Trust plays a critical role in technology adoption. Buecker et al., (2008) defined trust as the expression between parties that one party to a relationship agrees to believe statements made by another party. Trust is an aggregation of history, experience, and risk tolerance (Buecker et al., 2008). In FIM, trust management addresses relationships between users, service providers, and identity providers. Trust has a critical role in encouraging consumers to adopt the new innovative technology.

Despite the potential business value FIM presents, there is still skepticism among organization executives about accepting this technology. Even though trust is a critical part of the identity management process, this aspect of the FIM process has not received sufficient attention. Experts in various fields of study view trust with diverse viewpoints; however, there are some shared prospects. Trust involves two participants: the trustor and the trustee (AlQatan et al., 2012). Building trust may require some element of risk, but trustors have confidence that trustees will not betray their risk-assuming behavior (Meng, Min, & Li, 2008). Figure 11 shows the trust relationship between identity and service providers.

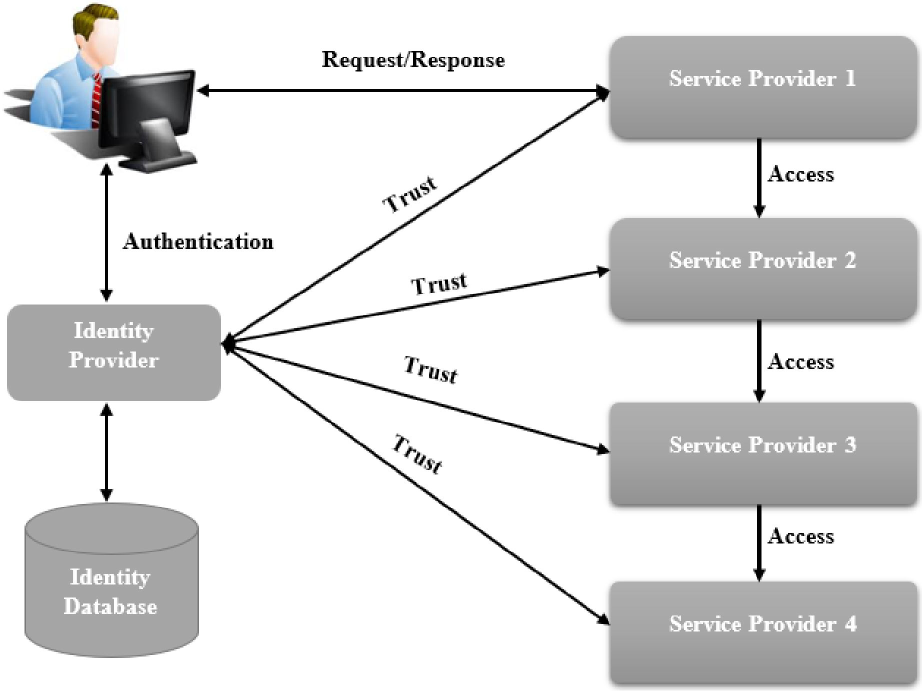


*Figure 11*. Trust relationship between identity and service providers

One of the significant challenges of FIM is the management of trust relationship among the federated partners and ensuring all trusted partners are living up to their promise. All trusted parties must adhere to the security and privacy standards that make federation work. The federation identity builds on the autonomy of domain entities having their own identity and privilege systems. Federated identity management allows one organization to trust another organization's user-access assertions and to permit access to applications and other resources. Because of the degree of autonomy of the domain entities, FIM stores credentials at both organizations; subscribers enter their login credentials once to access one or multiple domains.

**Trust framework components.** The trust framework consists of rules and policies that govern how federating members operate and interact (Temoshok & Abruzzi, 2016). The trust components include identity management responsibility; sharing, using, and protecting identity information; and managing liability and legal issues about federation members. To establish and maintain a trust relationship, federated partners can limit federated users' activity by implementing technical and procedural solutions, monitoring the security of the domain partners, and ensuring the establishment of a legal agreement (Temoshok & Abruzzi, 2016). Figure 12 shows the component of trust framework.

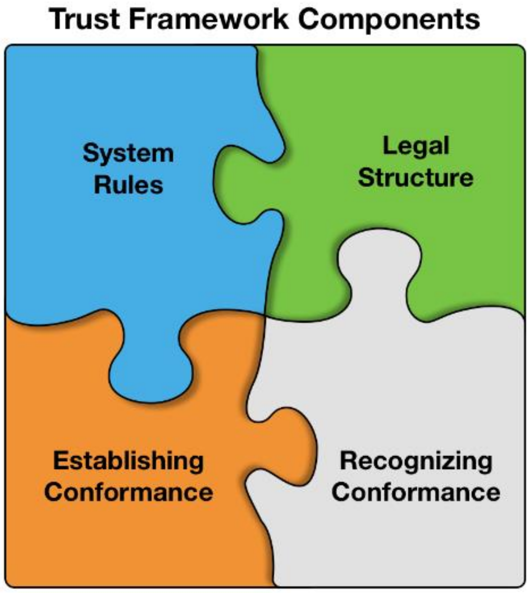


*Figure 12*. Trust framework component. Reprinted from Developing Trust Frameworks to Support Identity Federations, p. 7, by D. Temoshok & C. Abruzzi, 2016, National Institute of Standards and Technology.

***System rules*.** System rules according to Temoshok and Abruzzi (2016) involve governing community members' interactions by specifying the operation and technical requirement to preserve the federation identity and also prescribe the roles and responsibility for executing that operation. System rules involve registration and enrollment process activities, identity proofing, credential management based on risk, privacy requirements, security and data handling requirements, and technical specifications (Temoshok & Abruzzi, 2016).

***Legal structure.*** Temoshok and Abruzzi (2016) defined the legal structure as the rights, responsibilities, and liabilities of the federation participants. The legal structure presents a legal framework through a contract or a memorandum of understanding to bind operation and technical requirements to the federating members. Trust frameworks must be established within the framework of public laws and should be applied within the boundary of the member operations (Temoshok & Abruzzi, 2016). For example, federation members can build their legal framework on the following public laws:

- Child Online Privacy Protection Act: Designed to protect the privacy of children under 13 years of age from online service providers.
- Financial Services Modernization Act (Gramm-Leach-Bliley Act): Regulates the financial institutions regarding the collection, use, disclosure, and safeguarding of financial information (Temoshok & Abruzzi, 2016).
- Health Insurance Portability and Accountability Act: Designed to protect sensitive patient data.
- Fair Credit Reporting Act: This act was created to promote accuracy, fairness, and privacy of the information recorded and retained by the consumer reporting agencies (Fair Credit Reporting Act, 2012).

***Establish conformance.*** Federation members must establish and enforce conformance to a set of agreement and operating rules among members. Establishing conformance is the method through which federation members evaluate their processes and systems against the agreed-upon requirements of a trust framework (Temoshok & Abruzzi, 2016). Each federating member must demonstrate conformance within an identity federation. Federation members must base compliance efforts on the degree of risk and the magnitude of harm resulting from the confidentiality, integrity, and availability of a participant member's data. Depending on the federation administrator's risk appetite, organizational leaders may decide to conduct their self-assessment or leverage a third-party assessment organization audit.

***Recognizing and communicating conformance*****.** Recognizing and communicating conformance is the final process and the platform for communicating the completion of the conformance. Federating communities can also view a list of service providers deemed compliant with rules and requirements through registries and listing services. For example, the U.S. government initiated a government-wide Federal Risk and Authorization Management Program (FedRAMP). This program provides "a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" (General Services Administration, 2012, p. 2). It is a marketplace dashboard that provides a searchable, sortable database of all cloud services that received authorization from the Federal Risk and Authorization Management Program (FedRAMP, 2017).

Various researchers have proposed solutions to address the issue of trust with regards to FIM (Alpár, Hoepman, & Siljee, 2011; Premarathne, Khalil, Tari, & Zomaya, 2017). Managing numerous credentials for accessing organization resources or services will continue to present security challenges. Trust is one of the critical issues in an open environment, and a lack of trust between these entities may lead to security concerns. The current FIM framework is poorly defined or out of specification scope and sometimes too rigid to allow an agile and secure way to establish relationships (Cabarcos et al., 2014).

One of the significant flaws identified in the OAuth was that the protocol offered no unlinkability between the identity provider and the relying party regarding requests for the identity or data of a user (Isaakidis et al., 2016). Many researchers have challenged the issue of blanket trust given to identity providers. For example, identity providers provide authoritative information on behalf of a user. Isaakidis et al. (2016) discovered several instances where identity providers have collected detailed data on user behavior by logging the transactions between itself and relying parties on a per-user basis. To address this shortcoming, Isaakidis et al. developed a privacy-enhanced solution commonly known as UnlimitID. This solution leveraged lightweight attributes based on anonymous credentials founded on algebraic message authentication codes to preserve the privacy of users. The solution allowed the creation of multiple persistent and unlinkable pseudo-identities (Isaakidis et al., 2016). However, the approach only allows changes to the identity provider and the client but does not require any modification to the deployment code of the relying parties.

Ahmad Khattak, Ab Manan, and Sulaiman (2012) developed a proof of concept Trustworthy Mutual Attestation Protocol as a solution for the local true SSO leveraging of the Integrity Measurement Architecture with the Trusted Platform Module to gain user confidence. In the Ahmad Khattak et al. proposed solution, the trusted entity assumes the role of the authentication service provider between distinct service providers.

Pérez-Méndez, Pereñíguez-García, Marín-López, and López-Millán (2012) proposed a secure educational roaming technology called EDUROAM based on 802.1X architecture and a hierarchical RADIUS-based infrastructure. Pérez-Méndez et al. developed EDUROAM for international research and education community to provide roaming network access across research and education networks. This secure network federation allows EDUROAM member institutions to leverage their local institution credentials to access the Internet while visiting other institutions. Since EDUROAM capability can only support the user authentication and primary authorization process, Pérez-Méndez et al. initiated another project to improve the federation network by incorporating deploying authorization mechanisms. With the support of Kerberos, an authentication protocol, the deploying authorization mechanisms for federated services in EDUROAM architecture permits authenticated users into the network to have additional access to federated application services without deploying additional cross-realm infrastructures (Pérez-Méndez, 2012).

## Privacy Concerns

Privacy is defined as “the rights and obligations of individuals and organizations concerning the collection, use, retention, disclosure, and disposal of personal information” (American Institute of Certified Public Accountants, 2011, p. 1). Laudon and Traver defined privacy as “the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state” (as cited in Alkhalifah & Amro, 2017, p. 176).

Since the advent of the Internet, online users have had privacy concerns about the use, storage, disclosure, and dissemination of their data and sensitive information. Privacy has become a significant concern. Researchers have shown that privacy concerns have a direct influence on users’ behavioral intentions in various settings, including the influence of privacy identity management systems (Alkhalifah & Amro, 2017), e-commerce (Inman & Nikolova, 2017; Malhotra, Kim, & Agarwal, 2004), and social networking communities (Fogel & Nehmad, 2009; Shin, 2010). Sheng, Nah, and Siau (2008) examined the influence of privacy on e-commerce, electronic health records (Angst & Agarwal, 2009; Kenny, 2016), and location-based services (Xu & Gupta, 2009). Most of these researchers examined privacy concerns as a single construct. Although many researchers have investigated the effect of privacy concerns on technology adoption, not many studies exist on FIM adoption.

To address the issue of privacy concerns, Alkhalifah and Amro (2017) developed a model of how multidimensional privacy concerns affect users' adoption of identity management systems. Alkhalifah and Amro asserted that behavioral intention is a critical variable in determining identity management system adoption. Alkhalifah and Amro categorized privacy concerns into seven dimensions: collection, improper access, error, secondary use, control, awareness, and choice. The dimensions offer insights into users' privacy concerns. Alkhalifah and Amro suggested organizational leaders should consider the dimensions of privacy when designing privacy-enhancing identity management systems.

Birrell and Schneider (2013) focused on identifying critical design choices that are essential to FIM. The study involved exploring the connection between design choices and discussed the effect of their decision on system functionality. Birrell and Schneider adopted a privacy-driven approach that focused on three privacy properties: undetectability (i.e., the ability to conceal a user's action), unthinkability (i.e., the ability to conceal correlations between actions and identities), and confidentiality (i.e., the ability to control information dissemination).

In a study on the validity of privacy challenges in federated identity, Nuñez and Agudo (2014) proposed BlindIdM, a privacy-preserving model for Identity Management as a Service in the cloud. Nuñez and Agudo developed the proposed solution to address the overwhelming concerns of organizational leaders about the loss of control over outsourced data. The study leveraged the SAML 2.0 identity management protocol and proxy re-encryption to achieve data confidentiality with regards to the cloud provider.

Ahmad Khattak et al. (2012) developed a prototype and performance evaluation for the Trustworthy Mutual Attestation Protocol for a local true SSO system. The study involved conducting a reliability and validity test by constructing practicable security, trust, and privacy framework that integrated a standard federated identity and access management system using trusted computing. The findings indicated the importance of establishing trust before any transaction can take place.

## Security Concerns

One of the primary objectives of FIM is to improve user security by relieving users from having to remember several credentials due to the SSO feature (M. Wolf, Thomas, Menzel, & Meinel, 2009). Technology innovation has exposed organizations to increased and constant threats from opening enterprise security domains through web-based access (Senk, 2013). Security concerns are one of the challenges of FIM adoption. The most prominent concern in many organizations is the fear that unauthorized users can access and take control of their operation (Jensen & Jaatun, 2013). The fear is that an unauthorized user can impersonate the legitimate user to gain access to all the organization where this user has access rights (Jensen & Jaatun, 2013).

This concern led the Provisioning Service Technical Committee to incorporate new standards called Service Provisioning Markup Language (SPML) and SAML. These two protocols are OASIS standards and XML-based protocols. Most organizations accept version 2.0 of SPML. SPML is an open standard based on the concept of Directory Service Markup

Language for exchanging user, resource, and service provisioning information while SAML is a standard for secure exchange of authentication and authorization data between security systems of the cooperating organizations (Khara & Gupta, 2017).

Although numerous researchers have proposed various techniques, methods, and policies to protect users' identity information, several vulnerabilities exist. Somorovsky, Mayer, Schwenk, Kampmann, and Jensen (2012) examined 14 SAML standard models and identified several flaws related to XML signature wrapping. Somorovsky et al. discovered some of the SAML protocols had critical XML signature-wrapping vulnerabilities and proposed an automated penetration testing tool for XML signature wrapping.

Wang, Chen, and Wang (2012) conducted a security analysis on Microsoft Passport, OpenID 2.0, and SAML 2.0 and detected critical local flaws in the SSO system in browser-related messages. Wang et al. revealed a widespread security vulnerability related to OAuth implementation that allows attackers to gain unauthorized access to companies' data remotely. Remote attackers can substitute their credentials with the victim's credential during the OAuth exchange process.

Federated identity management is not immune to phishing attacks. Like the traditional identity management solution that usually fails to handle phishing attacks, FIM might be at risk if attackers compromise the SSO credentials to steal an identity. As a result, a phishing attack can manipulate victims into exposing sensitive enterprise information (Ahmad Khattak et al., 2012). For example, researchers at Kaspersky Lab (2015) detected phishing attacks that could give scammer's access to Microsoft Live IDs through a security vulnerability in the open protocol for authorization. Attackers can then gain unauthorized access to personal and sensitive information stored in users' profiles.

## Perceived Risk

Concerns about risk in FIM are growing. Perceived risk is a fundamental concern of decision-making process particularly in the technology adoption, and it is driven by expected internal resistance (Masoud, 2013; Senk, 2013). Perceived risk is a potential for loss or peril as a result of adopting FIM. For this study, perceived risk is a disclosure of personal information when using FIM which causes users to be pessimistic about future impacts of such disclosure. Perceived risk is a significant influence in preventing the adoption intentions of consumers (Claudy et al., 2015; Kleijnen et al., 2009). The growth of the Internet and the resulting interconnectedness of networks has exposed organizations to Internet-based attacks and highlighted multiple cases of the theft of intellectual property and business secrets and breaches of personal and sensitive information by hackers.

Despite the benefits of FIM over the traditional authentication solutions and foreseeable opportunity for future growth, however, this technology still faced with some challenges. Perceived risk plays a critical role in consumer adoption decision making and a valuable contributory factor towards explaining information-searching behavior and consumer purchase decision making (Masoud, 2013). Perceived risk is anchored on two theoretical perspectives, the first is focused on a decision result's uncertainty and the second is on the costs or consequences of such decisions (Masoud, 2013).

Many factors can influence user adoption of FIM. In most of the time, users often appraise the perceived benefits against the associated risks before making decisions. It is imperative that the identity service providers provide users with adequate information to enable them to make informed adoption decisions. User concern on perceived risk ranges from fear of losing access to multiple accounts, learning new authentication paradigm, high potential for loss resulting from disclosing personal information to the service provider, identity service provider trustworthiness and misuse of sensitive information by the service provider can negatively influence adoption of FIM (Grassi et al., 2017).

Earlier empirical studies on perceived risk mostly included a focus on consumer behavior on product and service evaluations and purchases. For example, Savas (2017) investigated the influence of various facets of perceived risk and consumer adoption of service innovations. Savas affirmed the neglect of three aspects of relationships in the perceived risk and consumer adoption of innovations: (a) most researchers had focused on products with little attention to services, (b) few researchers examined perceived risk as a multidimensional construct, and (c) researchers excluded consumer characteristics in most innovation studies.

Xu (2013) examined the adoption of theme park wait-time apps from the user's perspective. The study included gain and loss factors as the mediating variable that influences customers' perceived value on behavioral intention to adopt wait-time apps. Xu affirmed that perceived risk and the perceived fee had a significant impact on intention to adopt wait-time apps. Xu also discovered a significant difference in behavioral intention between users and nonusers of wait-time apps to adopt wait-time apps in the future. In FIM, organizational leaders cannot underestimate the issues of perceived risk, as who collects transactional data is a primary concern. Another concern was who sets the rules of authentication, what happens when things go the other way and who gains and who loses from interoperability (Jensen & Jaatun, 2013)?

## Critique of Previous Research Methods

The researcher conducted the literature review to examine the strengths and weaknesses of the various methodologies used by researchers to examine the subject. The information gathered served to guide the researcher toward a methodology that could deliver a meaningful conclusion that was both replicable and generalizable. Various researchers have used quantitative and qualitative research methods to study the same phenomena. The researcher observed that various research methodologies used in the literature review to study the FIM offered a varied but comprehensive view of the phenomenon of FIM. Some qualitative studies lacked objective data. The qualitative research method has received criticism regarding its poor validity and reliability due to the subjective nature, origin, and original contexts of qualitative data, which means it is impossible to replicate qualitative studies (Carr, 1994).

Past and current studies on FIM lack empirical research. For example, Alkhalifah and D'Ambra (2015) noted that a majority of the studies on FIM are descriptive and include intuition-based reasoning and conceptual analysis instead of empirical investigations. Therefore, research efforts should include a focus on empirically based research to develop theories. In some of the studies reviewed, authors noted insufficiency of a theoretical foundation of FIM and used a grounded theory approach to develop a theoretical model, noting that existing theories and models are not readily transferable to the context of FIM.

The researcher observed low variability of data quantity in the literature reviewed. The study, therefore, required a large sample to produce a more accurate analysis and hence to generalize the study findings to broader populations. Small samples may not be reliable because of the lack of data. The researcher further observed a confirmation bias in several studies where the authors used a single survey tool, such as Survey Monkey, Survey Gizmo, and Qualtrics, as the variable data source in one instrument. Research has shown that leveraging a study on a single method of data collection is likely to lead to a biased study. The literature revealed that some researchers did not apply common method variance (CMV) to minimize the source of bias during an experiment's design, as the design of a survey instrument can cause researchers to bias their responses.

In this study, the researcher identified some specific strengths in the validity of instruments, such as test-retest, equivalent forms, split halves, interrater, internal consistency, and reliability indicators. Results of quantitative studies on assessments of structural models revealed the acceptance or rejection of the stated hypotheses. The researcher presented the hypotheses and linked the hypotheses to the purpose of the study, the research question, and the methodology of the study. The process of calculating the reliability values for each subfactor in most studies involved using Cronbach's α, with all results above 0.80, which is higher than the recommended minimum value of 0.7 (Field, 2013).

## Summary

This chapter included a comprehensive review of the pertinent literature to outline the intellectual progress of research on FIM adoption. The literature review showed that the introduction of FIM would bring some value to organizations. The study revealed high expectations among researchers regarding what FIM can deliver and the benefits of adopting FIM solutions. However, the challenges to overcome before attaining the promises of FIM with optimal results are considerable.

Researchers of many FIM studies have overemphasized the importance of trust, privacy, security, perceived risk, investment cost, assurance, interoperability, revocation, knowledge, and data synchronization and consistency, and each converges on particular issues or on viewing the problem from a functional perspective (Alkhalifah & D'Ambra, 2015; Jensen, 2012). Some of these studies centered on technical or design problems and challenges of FIM. The findings revealed a lack of behavioral research in the FIM field. Seltsikas and O’Keefe (2010) noted a divergent view of FIM and claimed that having a goal of achieving a single conceptualization of the concept is ambitious. Additionally, the researcher did not fully explore the research on FIM from the perspective of users, and researchers have not discovered a suitable framework for understanding FIM from both business and users’ perspectives (Jensen, 2012; Satchell et al., 2011; Seltsikas & O’Keefe, 2010). Few researchers have discovered and proposed some factors and metrics toward the adoption of FIM (Ghazizadeh et al., 2012; Hackett & Hawkey, 2012; Haghshenas & Seyyedi, 2012; Jensen, 2011; Jensen & Jaatun, 2013). No researchers had examined the proposed theoretical models or empirically tested factors affecting user adoption of FIM. Hence, researchers recommend more studies on survey users’ perceptions of FIM (Ghazizadeh et al., 2012; Hackett & Hawkey, 2012; Haghshenas & Seyyedi, 2012; Jensen, 2011; Jensen & Jaatun, 2013).

The findings and analysis of this review contribute to the field of organizational management and technology adoption literature by providing evidence that scholar-practitioners can use to understand the phenomenon of FIM. The findings are particularly relevant to practitioners who wish to adopt FIM in their organization or want to understand how to manage the trend that has appeared in their enterprise without their knowledge or permission.

Chapter 3 includes the purpose of the study, research question, hypotheses, and research design. The chapter also includes a description of the population and sample, power analysis, procedures, participant selection, protection of participants, data collection, data analysis, validity of instruments, and reliability of data. Also discussed are the ethical considerations.

# CHAPTER 3. METHODOLOGY

Chapter 3 includes the purpose of the study, research question, hypotheses, and research design. The researcher defines the target population and sample, including the power analysis conducted to determine the size of the sample. The researcher also describes the methodology for data collection and data analysis. Within the data analysis section, the researcher provides the descriptive statistics used to describe the latent variables in the research question and the sample, along with the statistical methods using partial least squares structural equation modeling (PLS-SEM) and multiple regression to test the research hypotheses. The researcher also describes the validated survey instrument, as well as validity and reliability data for the instrument. Finally, the researcher presents the ethical practices employed to ensure the protection of the participants.

## Purpose of the Study

The purpose of this quantitative correlational research was to investigate the extent that the dimensions of trust (security, privacy, and perceived risk) relate to the behavioral intentions to adopt FIM, in conjunction with the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business. The goal was to advance the UTAUT body of knowledge and extend the applicability of UTAUT2 to FIM, which is a task not attempted by Venkatesh et al. (2003). Venkatesh et al. overlooked trust, security, privacy, and perceived risk in the initial UTAUT model (Im et al., 2008). Earlier studies revealed that trust, security, privacy, and perceived risk are the most crucial factors to consider in technology acceptance (Lee et al., 2010). This study involved examining the relationship between trust, security, privacy, and perceived risk and the constructs of UTAUT. The research provides an understanding of how trust, security, privacy and perceived risk, relates to the original UTAUT core constructs (Lee et al., 2010; Venkatesh et al., 2012).

## Research Questions and Hypotheses

**RQ1.** To what extent do the dimensions of trust (security, privacy, and perceived risk) relate to the behavioral intentions to adopt FIM, in conjunction with the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business?

**$H1_0$:** There is no correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**$H1_a$:** There is a correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**$H1_{01}$:** There is no correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**$H1_{a1}$:** There is a correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**$H1_{02}$:** There is no correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**$H1_{a2}$:** There is a correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03}$:** There is no correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03a}$:** There is a correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

## Research Design

This research study involved employing a quantitative, nonexperimental correlation and cross-sectional design approach to examine the effect of trust and UTAUT constructs on behavioral intention to adopt FIM using inferential statistical models to test hypotheses and answer the research question. The cross-sectional design is suitable for comparing different population groups at a single point in time, for demonstrating correlations between research variables, and for generalizing from a sample to a target population (De Vaus, Gray, Qu, & Stanton, 2010). The study included a single data collection method with IT decision makers in U.S. business. The researcher used a survey as the primary instrument for investigating trust as a predictor for adopting FIM by IT decision makers. The participants for this research study were IT decision makers from U.S. businesses. The researcher administered the survey instrument of Zhou (2012) and Opala (2012) to randomly selected participants.

The researcher employed Qualtrics, a professionally administered survey system, for data collection. The researcher provided the survey instruments and sampling criteria to the Qualtrics account manager who distributed them to randomly selected participants who met the criteria, which yielded 168 completed questionnaires. The researcher obtained informed consent from all the randomly selected participants before the gained access to the survey. Qualtrics sent and retrieved the questionnaires. The Qualtrics account manager anonymized the responses by removing all personally identifiable information such as names, addresses, e-mail addresses, and phone numbers before providing the coded data to the researcher to protect the participant’s privacy. The researcher stored the data set on a full-disk-encryption hard drive on a biometrically protected Surface Pro 4 laptop.

## Target Population and Sample

As organizational leaders continue to seek centralized and automated solutions to facilitate secure access to enterprise resources among cooperating partners in mixed information technology settings, it was appropriate to study user adoption of FIM by persons employed in organizations within the United States. Given this target population, Qualtrics provided an unbiased, randomly selected, and accessible demography for the sample frame that met the sampling criteria established for the study.

### Population

The population of interest for this study consisted of chief information officers, chief technical officers, IT project managers, enterprise architects, and IT directors. The researcher randomly sampled each of these roles from the population of U.S. business. The researcher employed Qualtrics, an online survey company, for data collection to provide a quantitative description of the trends, attitudes, or opinions of IT decision makers in U.S. business (Creswell, 2009). The principal sources of information for this study were IT decision makers who worked in U.S. business. The criteria for participation included individuals with IT expertise, chief information officers, chief technical officers, IT project managers, enterprise architects, IT directors, and anyone responsible for making IT decisions. The researcher carefully selected the sampling technique and sample size, as they performed a critical role in the selection of research participants. The researcher analyzed age, gender, job role, and technical experience, as well as participants' level of education based on the data.

**Sample**

The researcher based the recruitment strategy and sampling method on previous studies, in particular, the original constructs of the UTAUT (Zhou, 2012) and trust constructs (Opala, 2012). The researcher validated and inspected all the previous measures for the predictors to ensure reliability. The sample most suitable for this study was IT decision makers within organizations who were using or intended to use federated identity solutions. This sampling frame represented a section of the population that had a reasonable chance of selection in the sample. The inclusion criteria for the sampling frame for this study included IT decision makers between 21 and 70 years of age in the United States who are familiar with FIM technology. The process of computing the minimum required sample size involved using GPower 3.1.9.2 software, with the parameters being a power of 0.95, an effect size of 0.15, a medium scale, and an alpha level or level of significance of .05. By considering multiple linear regressions as the primary statistical tool and using eight maximum predictors, the minimum required sample size was 160 based on a 95% confidence interval.

As the researcher planned to employ SEM as the primary data analysis technique to test the research hypotheses, determining the proper sample size have a significant role in developing and understanding the results of SEM analysis. Determining the sample size requirement for SEM is a challenge for many researchers. Due to advancements, flexibility, and ease of use in the statistical modeling approach, the number of researchers using latent variable analyses and has increased, which also raises questions about how to estimate the necessary sample size for testing such models (Wolf, Harrington, Clark & Miller, 2013). Several researchers have proposed a rule of thumb for estimating sample sizes for SEM studies. For instance, Boomsma (1985) recommended a minimum sample size between 100 and 200, Bentler and Chou (1987) suggested a minimum of five or 10 observations per estimated parameter, and Nunnally (1967) recommended 10 cases per variable. However, these recommended rules were not model specific and may lead to grossly over- or underestimated sample size requirements (Wolf, et al., 2013). Some authors have contended that researchers can test simple SEM models, even if the sample size is quite small (Hoyle, 1999; Marsh & Hau, 1999). Other authors have recommended 100–200 should be the minimum sample size for conducting SEM (Anderson & Gerbing, 1988; Boomsma & Hoogland, 2001; Kline, 2005; Tabachnick & Fidell, 2007; Tinsley & Tinsley, 1987).

This study had nine variables, and according to the rules of thumb, the minimum sample size for this study was 160. As a method of comparison with prior studies, the sample size was consistent with the sample size of 191 used by Zhou (2012) and the sample size of 215 used by Venkatesh et al. (2003). The selected sample size of 160 was also consistent with prior similar studies and would have been sufficient for answering the research question. The researcher designed the survey in such a way to achieve the target sample size.

**Power Analysis**

The sample size of 160 was the result of using G*Power 3.1.9.2 (Faul, Erdfelder, Buchner, & Lang, 2009), assuming an a priori power analysis, $\alpha = .05$, $\beta = .95$, and medium effect size (0.15). An *F* test was the test family for the omnibus hypothesis using multiple linear regression, fixed model, $R^2$ deviation from zero. The results of the G*Power, a priori analysis, are in Table 1.

Table 1. G*Power Sample Size Calculation

| Input Parameters | Output Parameters | |
|---|---|---|
| Effect size f² = 0.15 | Noncentrality parameter λ = | 24.0000000 |
| α err prob = 0.05 | Critical F = 2.0002077 | |
| Power (1-β err prob) = 0.95 | Numerator df = 8 | |
| Number of predictors = 8 | Denominator df = 151 | |
| | Total sample size = 160 | |
| | Actual power = 0.9506385 | |

## Procedures

This section includes a description of the procedures for participant selection, data collection, data analysis, and the protection of participants in the study.

### Participant Selection

The researcher used inclusion criteria such as, IT decision makers between 21 and 70 years of age in the United States who are familiar with FIM technology to select representatives of the population for this survey. The Qualtrics membership pool, called Audience are IT decision makers between the ages of 21 and 70 years, served as a simple random sampling tool to identify potential survey participants' availability through an e-mail link. Qualtrics then added to the sample Audience members who confirmed their willingness to participate in the study after providing informed consent. To ensure an appropriate sample size of 160 (see Table 1), the researcher contracted with Qualtrics to receive 160 completed surveys. The researcher used the force response validation for all multiple-choice questions. The forced-response is a feature in Qualtrics that prevent respondents from skipping through the questionnaire or force the participants to answer the survey questions before exiting the page (Qualtrics, n.d.). The goal of the data collection was to obtain a sufficient number of completed questionnaires to fulfill the required sample size. The researcher also inserted a commitment question at the beginning of the questionnaire that involved asking the participants to commit to providing high-quality data. This method helps reduce the number of invalid responses.

### Protection of Participants

The Qualtrics service provider randomly selected enough participants based on the sampling criteria to yield 160 completed questionnaires. The researcher obtained informed consent from all chosen participants before granting access to the survey. Qualtrics sent and retrieved completed questionnaires from the survey panel. To maintain the anonymity of participants, Qualtrics anonymized the responses by removing all personally identifiable information such as name, address, and IP addresses before providing coded data to the researcher. The researcher stored the data set on a full-disk-encryption hard drive on a biometrically protected Surface Pro 4 laptop.

### Data Collection

The researcher employed random sampling to gather data from various IT decision makers across the United States. The sampling demography was IT decision makers between the ages of 21 and 70. The researcher included a screening question at the beginning of the survey to screen out participants who had switched roles within an organization and no longer met the criteria to participate in the study. Out of 208 questionnaires sent to various IT decision makers across the country, Qualtrics collected 168 valid surveys after removing invalid and incomplete responses. 17 participants were screened out at the no-IT-authority question, five participants were screened out at the consent question, four participants were screened out at the speeder, i.e., finish too quickly, and 14 participants dropped out of the study partway through. The researcher used a questionnaire instrument with 5-point Likert-style measurements representing *strongly disagree*, *somewhat disagree*, *neither agree nor disagree*, *somewhat agree*, and *strongly agree*.

Data collection took place through Qualtrics, which is a commercial questionnaire administration service. Qualtrics conducted surveys online and used secure socket layer technology to collect and store data, as well as to provide other survey management functions securely. Using Qualtrics Audience, a service provided by Qualtrics, researchers can administer surveys explicitly to a targeted audience with defined demographic characteristics. Before collecting data, the researcher obtained permission from Zhou (2012) and Opala (2012) to use the survey instruments. The researcher also signed a written agreement with Qualtrics Audience. The study received approval from the Capella University Institutional Review Board (IRB) before collecting data. The researcher obtained IRB approval with Reference Number 2017-298 on March 23, 2017, and contacted Qualtrics to give the organization a description of the study, including the inclusion and exclusion criteria.

Next, the researcher created an account on Qualtrics and uploaded the validated survey instrument. After that, the researcher commissioned Qualtrics to administer the survey to the randomly selected sample from the sampling frame identified by Qualtrics Audience. Before activating the study, the researcher agreed on the additional details of the target population, such as the detailed description of the target population, the incidence rate, sample size requirement, the desired number of responses, and turnaround time. After that, the researcher administered the survey instrument to the randomly selected Qualtrics Audience sample. The researcher then uploaded the data collected into the Statistical Package for the Social Sciences (SPSS) for preanalysis data screening and subsequent data analysis. The anonymously collected data remained stored in a protected manner to prevent accidental deletions and unauthorized disclosures.

## Data Analysis

The researcher applied various statistical analysis techniques to analyze data, report, and answer the research question and test the hypotheses. The researcher used a regression analysis of latent variables based on the optimization technique of partial least squares to develop a model that represents the relationships between the researcher's nine proposed constructs (Sánchez-Alzate, & Sánchez-Torres, 2017). The PLS is a multivariate statistical method used in testing structural models to find the fundamental relationship between two matrices (Chin, 1998). Researchers can use PLS for theory confirmation, as it can indicate where relationships might exist and suggest propositions for testing later (Chin, 1998). PLS consists of three components: (a) a structural model, which reflects the relationships between the latent variables, (b) a measurement model, which shows the relationship between the latent variables and their indicators, and (c) the weighting scheme (Escobar-Rodríguez & Carvajal-Trujillo, 2014). The PLS technique is suitable for small samples and does not require any parametric conditions (Hullard, 1999; Ponte, Carvajal-Trujillo, & Escobar-Rodríguez, 2015). Data analysis for this study involved a two-stage approach to ensure the establishment of the data quality of the research model. The first stage was the development and evaluation of the measurement model, and the second stage involved the development of a full SEM. The SEM provides the flexibility to perform model relationships, construct unobserved latent variables, model errors, and statistically test a priori theoretical and measurement assumptions against empirical data (Chin, 1998; Tuan Mat, 2010).

## Preanalysis

***Data coding.*** The researcher did not perform a data coding activity, as the format used in Qualtrics is compatible with SPSS Version 24. The researcher imported the data collected into SPSS format.

***Handling of missing data and outliers.*** Missing data on questionnaires present potential challenges to researchers during data analysis. The issue of missing data arises when measurement instruments such as surveys fail, and the participant was unable to respond to all items (Mertler & Vannatta, 2013). To address missing data, the researcher introduced a forced response to validate all questions in the survey and to screen out incomplete or partial responses (i.e., from people who dropped out partway through). This method prevented the participants from skipping survey questions. The researcher examined the dataset using frequency distributions and descriptive statistics using the SPSS frequencies procedure.

Outliers are considered as cases with unusual or extreme values in a sample distribution that has the potential to affect the normality of data negatively (Field, 2013; Mertler & Vannatta, 2013). In this study, the researcher examined univariate outliers in SPSS® using the graphical method of box plots and identified multivariate outliers by conducting Mahalanobis distance analysis. Mahalanobis distance is defined as the distance of a case from the centroid of the remaining cases (Tabachnick & Fidell, 2007). Thus, it involves using standard scores to measure the point of separation of an instance of a variable from the middle of the distribution. The researcher evaluated the Mahalanobis distance as a chi-square ($\chi^2$) with the degree of freedom equal to the number of the variables in the analysis (Mertler & Vannatta, 2013).

***Descriptive statistics.*** The researcher performed descriptive statistics of the demographic variables using SPSS to determine the distribution of the data and other measures of central tendency. The researcher computed descriptive statistics such as frequencies and percentages on the demographic variables. For the continuous variables, the researcher calculated a combination of means and standard deviations to indicate the spread of data within the continuous variables.

***Testing of assumptions for structural equation modeling.*** The first assumption considered was the sample size for the study. Sample size plays a significant role in SEM because it affects researchers' ability to model complex relationships between multivariate data. Large sample sizes are necessary to obtain reliable parameter estimates. A standard rule of thumb is to have a sample size of more than 200, as 100 may be adequate, or a sample size that is at least 50 more than eight times the number of variables in the model (Tabachnick & Fidell, 2007; VanVoorhis & Morgan, 2007). The second assumption was that the relationships between the predictor and the dependent variables were linear. The third assumption was the data met multivariate normality. The fourth assumption was that the study achieved the homogeneity of variance, and lastly, multicollinearity was not present among the latent variables.

The researcher ensured the sample size was adequate, confirmed no missing data existed and eliminated all significant outliers. Also, the researcher tested linearity using a bivariate Pearson correlation. Finally, the researcher investigated the multivariate normality using the *z* values of the kurtosis and skewness, as well as P-P plots for all latent variables (Field, 2013).

**Measurement model.** The analysis approach centered on the two-step SEM method suggested by Anderson and Gerbing (1988). The researcher evaluated the measurement model to establish structural validity before developing the structural model for hypothesis testing. This method aimed to ensure the research model was valid, with the relationships well represented before testing the hypotheses. In the two-step model, the researcher first examined the measurement model to conduct confirmatory factor analysis (CFA) and model fit. The CFA involved testing (a) the reliability of the scale using Cronbach's alpha and composite reliability (CR) and (b) the validity of the scale using convergent and discriminant validity. The researcher evaluated model fit by examining the chi-square goodness of fit test statistic, comparative fit index (CFI), and goodness-of-fit index (GFI). The study also evaluated the normed fit index (NFI), and the root mean square of approximation (RMSEA).

**Structural model.** After the confirmation of the measurement model, the researcher then connected the latent variables to represent the relationships in the various hypotheses in a structural model (Hox & Bechger, 1998). This model, also developed using AMOS covariance-based SEM with maximum likelihood estimation, indicated the results of the hypotheses tests as well as the mediating relationship. The researcher used the universally accepted level of significance of *p* = .05 and presented the analysis of the hypotheses testing under the research question.

The research question was as follows: To what extent do the dimensions of trust (security, privacy, and perceived risk) relate to the behavioral intentions to adopt FIM, in conjunction with the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business? The researcher interpreted the results of the SEM hypotheses test for the following hypotheses:

**H1$_0$:** There is no correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**H1$_a$:** There is a correlation among the dimensions of trust (security, privacy, and perceived risk), UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**H1$_{01}$:** There is no correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{a1}$:** There is a correlation between security concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{02}$:** There is no correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{a2}$:** There is a correlation between privacy concern (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03}$:** There is no correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

**H1$_{03a}$:** There is a correlation between perceived risk (a dimension of trust) and behavioral intention to adopt FIM.

## Instruments

The instruments used for this study were the location-based technology acceptance and use of technology instrument developed by Zhou (2012) and cloud adoption developed by Opala (2012). The researchers developed the instruments based on the modified UTAUT theory. The researcher used the instruments as is, because they applied to this research, except for making a change in the name of technology from location-based services to FIM. Zhou's survey instrument included an adaptation of the eight most important constructs from prior studies. The basis of Opala's instrument was the previously validated study instruments of Venkatesh et al. (2003) to achieve construct measurement. Table 2 includes detail of the constructs in the Zhou (2012) and Opala (2012) instruments.

Table 2. Standardized item loadings for Zhou (2012) and Opala (2012)

| | | Item | | | | |
|---|---|---|---|---|---|---|
| Construct | Item | loading | AVE | CR | Alpha | Citation |
| Performance expectancy | PEE1 | 0.872 | 0.62 | 0.83 | .82 | Zhou (2012), adapted from Venkatesh et al. (2003) |
| | PEE2 | 0.780 | | | | |
| | PEE3 | 0.692 | | | | |
| Effort expectancy | EFE1 | 0.845 | 0.67 | 0.86 | .86 | Zhou (2012), adapted from Venkatesh et al. (2003) |
| | EFE2 | 0.816 | | | | |
| | EFE3 | 0.801 | | | | |
| Social influence | SOI1 | 0.742 | 0.64 | 0.78 | .77 | Zhou (2012), adapted from Venkatesh et al. (2003) |
| | SOI2 | 0.852 | | | | |
| Facilitating conditions | FAC1 | 0.747 | 0.58 | 0.81 | .81 | Zhou (2012), adapted from Venkatesh et al. (2003) |
| | FAC2 | 0.823 | | | | |
| | FAC3 | 0.714 | | | | |
| Privacy concern | PC1 | 0.783 | 0.7 | 0.9 | .90 | Zhou (2012), adapted from Son and Kim (2008) |
| | PC2 | 0.887 | | | | |
| | PC3 | 0.887 | | | | |
| | PC4 | 0.794 | | | | |
| Trust | TRU1 | 0.839 | 0.67 | 0.86 | .86 | Zhou (2012), adapted from Pavlou and Gefen (2004) |
| | TRU2 | 0.894 | | | | |
| | TRU3 | 0.717 | | | | |
| Perceived risk | RISK1 | 0.843 | 0.76 | 0.9 | .90 | Zhou (2012), adapted from Xu and Gupta (2009) |
| | RISK2 | 0.919 | | | | |
| | RISK3 | 0.843 | | | | |
| Usage intention | USE1 | 0.826 | 0.64 | 0.84 | .84 | Zhou (2012), adapted from Lee (2005) |
| | USE2 | 0.852 | | | | |
| | USE3 | 0.724 | | | | |
| Security | CS | 0.881 | 0.701 | 0.672 | .70 | Opala (2012), adapted from Venkatesh et al. (2003) |

*Note.* All data were ordinal. AVE = average variance extracted and CR = composite reliability

**Validity.** Opala (2012) used a validated instrument of Venkatesh et al. (2003) with discriminant, convergent, construct, and face validity based on the multitrait-multimethod matrix analysis of validity. The multitrait-multimethod matrix analysis was suitable to look for correlations between traits of different constructs and revealed a .90 correlation between each construct of perceived usefulness and ease of use in Venkatesh et al.'s study on wireless adoption. The study revealed a high, statistically significant intercorrelation between items or significant ($p < .005$) based on users' first acceptance of computer technology (Davis, Bagozzi, & Warshaw, 1989). Discriminant validity of the instrument shows the ability of the instrument to distinguish between measured objects. The researcher used construct validity to determine the actual measures by operationalizing the measurements presented in the instrument (Venkatesh et al., 2003). Discriminant validity showed loading patterns were acceptable, with the majority being at .70 or higher. The study maintained equal reliability and validity by integrating previously validated studies such as the TAM (Davis et al., 1989), diffusion of innovation (Rogers, 1995), and UTAUT (Venkatesh et al., 2003).

Validity in quantitative research indicates the degree to which the researcher measures concepts accurately (Heale & Twycross, 2015; Roberts, Priest, & Traynor, 2006). The suggested validity cut-off points were 0.3 for factor loadings and 1 for eigenvalues. When researchers modify existing instruments, they need to reestablish reliability and validity, but this study did not compromise established validity by adding security, cost-effectiveness, and IT compliance to the instrument to test for managements' perception of cloud adoption (Opala, 2012; Opala & Rahman, 2013).

Zhou (2012) conducted CFA to test the validity of the instrument. The result revealed that most item factor loadings were higher than 0.7, and *T* values indicate that all loadings were significant at .001. All average variance extracted (AVE) exceeded 0.5, and CR exceeded 0.7. Hence, the scale had good convergent validity. Also, all Cronbach's alpha values were higher than 0.7, which suggested good reliability. Zhou also tested discriminant validity by comparing the square root of AVE and factor correlation coefficients. The result revealed the square root of AVE is significantly larger than its correlation coefficients with other factors, which indicated good discriminant validity. Table 2 listed the standardized item loadings, AVE, CR, and Cronbach's alpha values for Zhou (2012) and Opala (2012).

**Reliability.** Zhou (2012) and Opala (2012) assessed the reliability of the data analysis using Cronbach's alpha to explain the means versus medians and ranks. Reliability is the ability of a measurement instrument to provide the same error-free results consistently. Testing for reliability to measure the degree to which an assessment tool produces stable and consistent results is a prerequisite for replicating research to get the same results (Cooper & Schindler, 2011). The reliability of the scales tested by Cronbach's alpha shows high reliability ($\alpha = 0.788$). The reliability coefficient ranges from 0 to 1, and a statistical value of .70 or better meets reliability requirements based on Cronbach's alpha (Field, 2013; Vogt, 2007).

## Operational Definition of Constructs

**Demographic variables.** The researcher observed all the demographic variables in the study. For example, gender was a binary categorical variable with 1 = male and 2 = female, age was a range of categorical data that included 1 = less than 21, 2 = 21–30, 3 = 31–40, 4 = 41–50, 5 = 51–60, and 6 = 61–70. Ethnicity was a binary categorical variable with 1 = White/Caucasian, 2 = American Indian, 3 = Asian, 4 = Hispanic/Latina, 5 = African American, 6 = Pacific Islander and 7 = other. Degree outside the United State was a binary categorical variable with 1 = yes and 2 = no. Annual household income was a range of categorical data with 1 = more than $20,000, 2 = $60,001–$80,000, 3 = $80,001–$100,000, 4 = $100,001–$120,000, 5 = 120,001–$140,000, 6 = $140,001–$160,000, 7 = $160,001–$180,000, 8 = $180,001–$200,000, and 9 = greater than $200,000. Also assessed was the approximate number of users supported by the organization as a range of categorical data from 1 = greater than 500, 2 = 501–1,000, 3 = 5001–10,000, 4 = 10,001–20,000, and 5 = more than 20,001. Years of experience making IT decisions for the organization was a range of categorical data from 1 = greater than 2, 2 = 2–5, 3 = 5–10, 4 = 10–15, 5 = more than 15 and 6 = others. Education was a categorical variable with 1 = less than high school/GED, 2 = associate degree, 3 = bachelor’s degree, 4 = master’s degree, 5 = doctoral degree, and 6 = other postgraduate degree. The primary major of the latest degree program the participant completed was a categorical variable with 1 = science, 2 = engineering, 3 = other technical, 4 = business, 5 = arts, and 6 = others. Finally, occupational title was a categorical variable with 1 = chief information officer, 2 = chief information security officer, 3 = director of IT, 4 = IT manager, 5 = IT team lead/supervisor, 6 = enterprise architect, 7 = vice president of IT, 8 = project manager, and 9 = other.

**Effort expectancy.** The researcher measured effort expectancy using three indicators from Zhou’s (2012) survey instrument. Zhou originally adapted this construct from Venkatesh et al. (2003). The three indicators for this latent variable were (a) learning to use FIM is easy for me (EFE1), (b) skillfully using FIM is easy for me (EFE2), and (c) I find that FIM is easy to use (EFE3).

**Facilitating conditions.** The researcher measured facilitating conditions using three indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Venkatesh et al. (2003). The three indicators for this latent variable were (a) I have the resources necessary to use FIM (FAC1), (b) I have the knowledge necessary to use FIM (FAC2), and (c) a specific person (or group) is available for assistance with FIM system difficulties (FAC3).

**Performance expectancy.** The researcher measured performance expectancy using three indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Venkatesh et al. (2003). The three indicators for this latent variable were (a) using FIM improves my living and working efficiency (PEE1), (b) using FIM increases my living and working productivity (PEE2), and (c) I find that FIM is useful (PEE3).

**Perceived risk.** The researcher measured perceived risk using three indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Xu and Gupta (2009). The three indicators for this latent variable were (a) providing this service provider with my personal information would involve many unexpected problems (PER1), (b) it would be risky to disclose my personal information to this service provider (PER2), and (c) there would be a high potential for loss in disclosing my personal information to this service provider (PER3).

**Privacy concern.** The researcher measured privacy concern using four indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Son and Kim (2008). The four indicators for this latent variable were (a) I am concerned that the information I disclosed to the service provider could be misused (PRC1), (b) I am concerned that a person can find private information about me on the Internet (PRC2), (c) I am concerned about providing personal information to the service provider because of what others might do with it (PRC3), and

(d) I am concerned about providing personal information to the service provider because it could be used in a way I did not foresee (PRC4).

**Security.** The researcher measured security using four indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Venkatesh et al. (2003). The four indicators for this latent variable were (a) I feel that FIM is secure (SEC1), (b) I am concerned about the security of the technology used in the FIM (SEC2), (c) I feel that FIM is more secure than the traditional authentication methods (SEC3), and (d) I am willing to use FIM to access sensitive information for my organization (SEC4).

**Social influence.** The researcher measured social influence using two indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Venkatesh et al. (2003). The two indicators for this latent variable were (a) people who influence my behavior think that I should use FIM (SOI1) and (b) people who are important to me think that I should use FIM (SOI2).

**Trust.** The researcher measured trust using three indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Pavlou and Gefen (2004). The three indicators for this latent variable were (a) this service provider is trustworthy (TRU1), (b) this service provider keeps its promise (TRU2), and (c) this service provider keeps customer interests in mind (TRU3).

**Usage intention.** The researcher measured usage intention using three indicators from Zhou's (2012) survey instrument. Zhou originally adapted this construct from Lee (2005). The three indicators for this latent variable were (a) I intend to use FIM in the next *n* months (BIA1),

(b) I predict I would use FIM in the next *n* months (BIA2), and (c) I plan to use FIM in the next *n* months (BIA3).

## Ethical Considerations

Ethics are norms or standards for distinguishing between right and wrong (Resnik, 2011). Ethical considerations are a critical aspect of research designs. In most times, ethics drive the direction of the research methodology. University-based researchers must seek IRB approval to conduct a study, especially when it involves human subject participation. The federal policy for the Protection of Human Subjects Regulations (2009) specified the conditions related to the requirements of an IRB review. The *Belmont Report* articulated three basic principles relevant to the ethics of research involving human participants: respect for persons, beneficence, and justice (Cassell, 2000). Researchers at the U.S. Department of Health and Human Services (1979) also mandated that researchers consider the rights and welfare of individual participants.

Respect for persons is the notion that all participants deserve the right to exercise full autonomy (Bell & Bryman, 2007). The Belmont Report incorporated at least two ethical convictions regarding respect for persons. The researcher understood the importance of ethics and the consequence of violations and adhered to the 10 principles of ethical considerations established by Bell and Bryman (2007), the Institutional Review Board, and the federal guidelines established by the Office for Human Research Protections of the U.S. Department of Health and Human Service. The researcher anonymized all individuals and organizations and obtained full consent before distributing the survey to the participants. The researcher removed all potentially confidential and sensitive information related to names, addresses, e-mail addresses, and phone numbers from the study. The researcher avoided any forms of deceit or overstatements regarding the aims and objectives of the research, and there were no instances of conflicts of interest through relationships and source of funding. The researcher communicated the potential risks and benefits of the study to the participants with truthfulness and transparency. The researcher also avoided any form of distorted information and did not demonstrate any biased opinion toward the primary data findings.

Respect for beneficence is considered the kind of respect accorded to the participants, i.e., making every effort not harming the participants (Gabriele, 2003). The researcher ensured the protection of the participants from harm and placed priority on the respect for the dignity of the research participants by obtaining full consent from the participants (Bell & Bryman, 2007).

Respect for justice is defined as a fair distribution of costs and benefits to potential study participants (Bell & Bryman, 2007). Respect for justice means that one group should not be responsible for the research bill while the other team reaps the benefits of the study. The researcher proportionately applied the principle of justice, the burdens, and the benefits to all participants.

## Summary

Chapter 3 included the purpose of the study, research questions, hypotheses, and research design. The chapter also included the target population and sample size, power analysis, procedures, participant selection, protection of participants, data collection, data analysis, validity of instruments, and reliability of the data. Also discussed were the ethical considerations. Chapter 4 includes a description of the findings related to the research question and hypotheses, the sample for the study, and assumptions.

# CHAPTER 4. RESULTS

## Background

Chapter 4 includes the findings of the research study. The basis of the findings for the research question and hypotheses derived from the predefined research problem and purpose. This chapter includes a description of the population and sample selected for the study with regards to the data collected, the handling of missing data, and data transformed in preparation for the data analysis phase. Included in this section are the findings from the demographic, exploratory, and descriptive analysis. The chapter also includes a brief description of the study results and findings, detailed explanations of the hypotheses testing using multiple regression analysis, and the results of each test. The researcher also discusses the process of evaluating the assumptions for the multiple regression models. The chapter closes with a summary of the study components and a restatement of the findings of the study.

## Description of the Sample

The researcher employed Qualtrics, a marketing research firm, to carry out the data collection exercise. The researcher conducted a cross-sectional descriptive correlation study with a national sample of eligible IT decision makers across U.S. businesses through the Qualtrics Panel to help gather the sample for the study, which ensured there was a full representation of the total population. During the data collection phase, Qualtrics obtained completed surveys from 168 participants.

### Data Coding

Based on the compatibility of the data formats in Qualtrics with SPSS, the researcher exported all the individual responses in Qualtrics to SPSS Version 24. In SPSS, the researcher then cleaned the data in preparation for data analysis, which involved examining the data labels, types, width, decimals, and values to make sure they were in the right formats. The researcher aggregated the cases and performed a reflection on a negatively skewed variable and log transformation by squaring the variable items that comprised each of the significant variables into composite variables for each measured construct using the compute-variable command in SPSS. Table 3 shows the coded data.

Table 3. Coded Data

| Section | Questions | Question numbers | Label |
|---|---|---|---|
| PEE | Performance expectance | 1-3 | Q1PEE–Q3PEE |
| EFE | Effort expectancy | 4-6 | Q1EFE–Q3EFE |
| SOI | Social influence | 7-8 | Q1SOI–Q2SOI |
| FAC | Facilitating intentions | 9-11 | Q1FAC–Q3FAC |
| TRU | Trust | 12-14 | Q1TRU–Q3TRU |
| SEC | Security | 15-18 | Q1SEC–Q4SEC |
| PRC | Privacy | 19-22 | Q1PRC–Q4PRC |
| RSK | Perceived risk | 23-25 | Q1RSK–Q3RSK |
| BII | Behavioral intention | 26-28 | Q1BII–Q3BII |

*Note.* All data were ordinal.

## Analysis of Missing Data and Outliers

Before conducting the SEM procedure, the researcher screened the survey data for possible missing data using missing value analysis. Data become missing when participants do not respond to a survey question or when there are omissions in the data collected. The output of the missing value analysis in Table 4 indicates that there were no missing values because the researcher introduced forced responses to validate all questions in the survey, which also screened out incomplete or partial responses, such as people who drop out partway through. This method prevented the participants from skipping survey questions. The researcher examined the dataset using frequency distributions and descriptive statistics using the frequencies procedure in SPSS.

Table 4. Missing Value Analysis

| Variable | Mean | Std. deviation | Missing | |
|---|---|---|---|---|
| | | | Count | Percentage |
| Performance expectancy | 12.4107 | 2.21679 | 0 | 0 |
| Effort expectancy | 12.1190 | 2.35682 | 0 | 0 |
| Social influence | 7.8095 | 1.60446 | 0 | 0 |
| Facilitating conditions | 12.5952 | 2.16736 | 0 | 0 |
| Trust | 12.7083 | 12.7083 | 0 | 0 |
| Security concern | 15.9345 | 2.55746 | 0 | 0 |
| Privacy concern | 14.3214 | 4.33247 | 0 | 0 |
| Perceived risk | 10.2440 | 3.45804 | 0 | 0 |
| Behavioral intention | 12.6071 | 2.29823 | 0 | 0 |

*Note*. *N* = 168.

Following the missing value analysis, the researcher attempted to identify possible outliers that have the potential to affect the normality of data negatively (Field, 2013; Mertler & Vannatta, 2013). Using boxplots is an efficient way to identify and provide necessary information about extreme values in a distribution. The researcher examined univariate outliers in SPSS using the graphical method of boxplots and identified multivariate outliers by conducting Mahalanobis distance analysis (Steven, 2001). Mahalanobis distance is the distance of a case from the centroid of the remaining cases (Cooper & Schindler, 2011; Tabachnick & Fidell, 2007).

The analysis of the boxplots in Figure 13 reveals four items in each of the variables of social influence and privacy and two outliers identified in facilitating conditions security. Using the outlier labeling rule introduced, the researcher further investigated the data. The analysis of the outlier labeling rule revealed four items identified in the variable of social influence, security, and privacy concerns. Accordingly, the researcher deleted the four outliers, which resulted in an updated sample size of 164 cases.

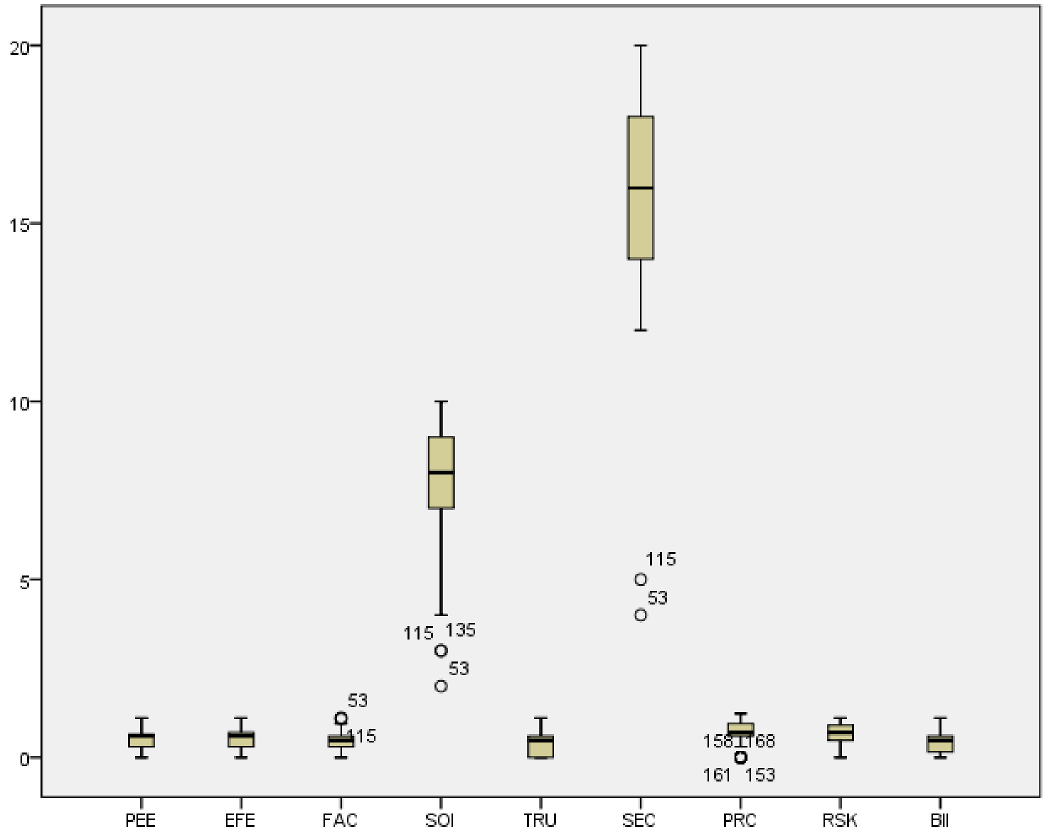


*Figure 13*. Boxplot chart for all the continuous variables

Following the identification of outliers using boxplots, the researcher used Mahalanobis distance analysis to identify the multivariate outliers and to remove the extreme outliers. The researcher evaluated the Mahalanobis distance as a chi-square with the degree of freedom equal to the number of the variables in the analysis (Mertler & Vannatta, 2013). According to Mitchell and Krzanowski (1985), Mahalanobis distance analysis is a suitable measure of distance between two distributions, which can significantly affect bias reduction in data analysis. Mahalanobis distance analysis involves using standard scores and assessing the proximity of a case from the center of the distribution (Hair, Black, Babin, Anderson, & Tatham, 2006).

Using SPSS, the researcher computed standard scores for each latent variable, and during the observation, a case was considered a multivariate outlier if the probability related to its Mahalanobis distance was ±3.0 or higher. Accordingly, from the analysis of the variables, 10 cases emerged as having a Mahalanobis distance of ±3.0 or greater. The researcher then deleted cases identified as outliers, so the final sample size after the deletion of outliers was 157 cases.

## Descriptive Statistics

The researcher conducted descriptive statistics on both the demographic variables and the continuous variables. The demographic variables considered were gender, age, household income, and highest education level completed. Respondents’ ages ranged from 21 to 70. Out of the 168 respondents, the age group most represented was 31–40 years (39%), followed by 21–30 years (35%), 41–50 years (16%), and 51–60 (10%), while the 61–70 years group was the least represented at 1%.

Table 5 shows the age-group distribution of respondents.

Table 5. Age Group Distribution of Respondents

| Age group | *n* | % |
|---|---|---|
| 21–30 | 59 | 35.1 |
| 31–40 | 65 | 38.7 |
| 41–50 | 27 | 16.1 |
| 51–60 | 16 | 9.5 |
| 61–70 | 1 | 0.6 |
| Total | 168 | 100.0 |

The gender distribution of respondents in Table 6 shows 87 male respondents (52%) and 81 female respondents (48%). The demographic information indicated that among the respondents, there were slightly more males than females, although the difference was not significant enough to skew the findings on a gender basis.

Table 6. Gender Distribution of Respondents

| Gender | n | % |
|---|---|---|
| Male | 87 | 51.8 |
| Female | 81 | 48.2 |
| Total | 168 | 100.0 |

The household income distribution in Table 7 reveals that 13 respondents had a household income between $20,000 and $60,000 (8%), 27 respondents had a household income between $60,001 and $80,000 (16%), 39 respondents had a household income between $80,001 and $100,000 (23%), 29 respondents had a household income between $100,001 and $120,000 (17%), 22 respondents had a household income between $121,001 and $140,000 (13%), and 13 respondents had a household income between $141,001 and $160,000 (8%). Also 11 respondents had a household income between $161,001 and $180,000 (7%), five respondents' household income was between $181,001 and $200,000 (3%), and nine respondents had a household income greater than $200,001 (5%). This distribution indicated a balanced spread of household incomes among respondents.

Table 7. Household income of respondents

| | *n* | % |
|---|---|---|
| $20,000–$60,000 | 13 | 7.7 |
| $60,001–$80,000 | 27 | 16.1 |
| $80,001–$100,000 | 39 | 23.2 |
| $100,001–$120,000 | 29 | 17.3 |
| $121,001–$140,000 | 22 | 13.1 |
| $141,001–$160,000 | 13 | 7.7 |
| $161,001–$180,000 | 11 | 6.5 |
| $181,001–$200,000 | 5 | 3.0 |
| Greater than $200,001 | 9 | 5.4 |
| Total | 168 | 100.0 |

The level of education of respondents shown in Table 8 indicates that respondents with bachelor's degrees had the highest representation (48%), followed by those with master's degrees (29%), and those with an associate degree (13%). Next were respondents with high school/GED or less (5%), while Ph.D. was 4% and others were 1%.

Table 8. Education of Respondents

| | *n* | % |
|---|---|---|
| High school/GED or less | 9 | 5.4 |
| Associate’s | 22 | 13.1 |
| Bachelor’s | 80 | 47.6 |
| Master’s | 49 | 29.2 |
| PhD | 6 | 3.6 |
| Others | 2 | 1.2 |
| Total | 168 | 100.0 |

The researcher also analyzed the descriptive statistics for each of the latent variables by calculating their means and standard deviations on a 5-point Likert-type scale. The subscales were performance expectancy (PEE), effort expectancy (EFE), social influence (SOI), facilitating conditions (FAC), trust (TRU), security concern (SEC), privacy concern (PRC), perceived risk (RSK), and behavioral intention (BII).

The mean for the PEE scale for the sample was 12.4107 on a 5-point scale with a standard deviation of 2.21679, which signified that most of the participants noted that using FIM would improve their job performance. The second subscale of EFE had a mean value of 12.1190 with a standard deviation of 2.35682, which indicated that most of the respondents considered FIM as easy to use and operate. The subscale SOI had a mean value of 7.8095 with a standard deviation of 1.60446, which indicated that most of the respondents believed that people whom they view as significant believe that they should use FIM. FAC had a mean of 12.5952 and a standard deviation of 2.16736, which signified a belief among the majority of the respondents that an organizational and technical infrastructure exists to support the use of FIM. TRU had a mean value of 12.7083 with a standard deviation of 12.70830, which showed that most respondents considered trust a factor in FIM usage. SEC had a mean value of 15.9345 with a standard deviation of 2.55746, which signified that some respondents expressed a security concern with using FIM. PRC had a mean value of 14.3214 with a standard deviation of 4.33247, which indicated that some respondents expressed privacy concerns by using FIM. RSK had a mean value of 10.2440 with a standard deviation of 3.45804, which signified a split between the respondents in their belief that using FIM may lead to the disclosure of their personal information, and the last subscale BII had a mean value of 12.6071 and a standard deviation of 2.29823. Table 9 shows the means and standard deviations for all these latent variables.

Table 9. Means and Standard Deviations for Latent Variables

| Variable | Mean | Std. deviation |
|---|---|---|
| Performance expectancy | 12.4107 | 2.21679 |
| Effort expectancy | 12.1190 | 2.35682 |
| Social influence | 7.8095 | 1.60446 |
| Facilitating conditions | 12.5952 | 2.16736 |
| Trust | 12.7083 | 12.70830 |
| Security concern | 15.9345 | 2.55746 |
| Privacy concern | 14.3214 | 4.33247 |
| Perceived risk | 10.2440 | 3.45804 |
| Behavioral intention | 12.6071 | 2.29823 |

*Note*. *N* = 168.

## Test of Assumptions for Structural Equation Modeling

The researcher investigated the assumptions for SEM by ensuring the sample size was large enough with no missing data or extreme outliers and the relationships between the predictor, and the dependent variables were linear. Other assumptions were that the variables are normally distributed, homogeneity of variance occurred, and there was no multicollinearity among the latent variables. In testing these assumptions, the sample size was consistent with the recommended large sample sizes and addressed the issues of missing data and significant outliers noted in earlier sections. The researcher also addressed the assumptions of linearity, normality, homogeneity of variance, and multicollinearity.

### Linearity

The researcher tested an assumption for linearity using bivariate Pearson correlation analysis. To meet the linearity assumption, the relationship between the predictor variables and the dependent variables should be linear (Field, 2013). As presented in the correlation matrix of the latent variables in Table 10, the correlation coefficients between each predictor and dependent variable show that at least 95% of relationships between the predictor and the dependent variables were statistically significant. The result of the linearity test indicated that there was no violation of the SEM linearity assumption between predictor and dependent variables and no data transformation was necessary.

Table 10. Correlation Matrix of Latent Variables

| | PEE | EFE | SOI | FAC | TRU | SEC | PRC | RSK | BII |
|---|---|---|---|---|---|---|---|---|---|
| Performance expectancy | | | | | | | | | |
| Pearson correlation | 1 | .673$^{**}$ | .562$^{**}$ | .659$^{**}$ | .617$^{**}$ | .554$^{**}$ | .195$^{*}$ | .151 | .613$^{**}$ |
| Sig. (2-tailed) | | .000 | .000 | .000 | .000 | .000 | .011 | .050 | .000 |
| Effort expectancy | | | | | | | | | |
| Pearson correlation | .673$^{**}$ | 1 | .464$^{**}$ | .621$^{**}$ | .587$^{**}$ | .604$^{**}$ | .301$^{**}$ | .271$^{**}$ | .542$^{**}$ |
| Sig. (2-tailed) | .000 | | .000 | .000 | .000 | .000 | .000 | .000 | .000 |
| Social influence | | | | | | | | | |
| Pearson correlation | .562$^{**}$ | .464$^{**}$ | 1 | .469$^{**}$ | .479$^{**}$ | .433$^{**}$ | .251$^{**}$ | .205$^{**}$ | .477$^{**}$ |
| Sig. (2-tailed) | .000 | .000 | | .000 | .000 | .000 | .001 | .008 | .000 |
| Facilitating conditions | | | | | | | | | |
| Pearson correlation | .659$^{**}$ | .621$^{**}$ | .469$^{**}$ | 1 | .618$^{**}$ | .544$^{**}$ | .213$^{**}$ | .165$^{*}$ | .572$^{**}$ |
| Sig. (2-tailed) | .000 | .000 | .000 | | .000 | .000 | .005 | .033 | .000 |
| Trust | | | | | | | | | |
| Pearson correlation | .617$^{**}$ | .587$^{**}$ | .479$^{**}$ | .618$^{**}$ | 1 | .530$^{**}$ | .221$^{**}$ | .127 | .659$^{**}$ |
| Sig. (2-tailed) | .000 | .000 | .000 | .000 | | .000 | .004 | .100 | .000 |
| Security concern | | | | | | | | | |
| Pearson correlation | .554$^{**}$ | .604$^{**}$ | .433$^{**}$ | .544$^{**}$ | .530$^{**}$ | 1 | .395$^{**}$ | .352$^{**}$ | .474$^{**}$ |
| Sig. (2-tailed) | .000 | .000 | .000 | .000 | .000 | | .000 | .000 | .000 |
| Privacy concern | | | | | | | | | |
| Pearson correlation | .195$^{*}$ | .301$^{**}$ | .251$^{**}$ | .213$^{**}$ | .221$^{**}$ | .395$^{**}$ | 1 | .698$^{**}$ | .220$^{**}$ |
| Sig. (2-tailed) | .011 | .000 | .001 | .005 | .004 | .000 | | .000 | .004 |
| Perceived risk | | | | | | | | | |
| Pearson correlation | .151 | .271$^{**}$ | .205$^{**}$ | .165$^{*}$ | .127 | .352$^{**}$ | .698$^{**}$ | 1 | .151 |
| Sig. (2-tailed) | .050 | .000 | .008 | .033 | .100 | .000 | .000 | | .051 |
| Behavioral intention | | | | | | | | | |
| Pearson correlation | .613$^{**}$ | .542$^{**}$ | .477$^{**}$ | .572$^{**}$ | .659$^{**}$ | .474$^{**}$ | .220$^{**}$ | .151 | 1 |
| Sig. (2-tailed) | .000 | .000 | .000 | .000 | .000 | .000 | .004 | .051 | |

*Note.* N = 168. **. Correlation is significant at the 0.01 level (2-tailed).

## Normality

The SEM assumption of the homogeneity of variance posits that the data should reflect a normal distribution. In this study, the values of the kurtosis and skewness, as well as the Q-Q plots for all latent variables, were suitable to test for normality. Using the kurtosis and skewness test, the kurtosis and the skewness for each latent variable should be between -1 and +1 to fulfill the normality assumption (Mertler & Vannatta, 2013). While testing the assumption using the Q-Q plot, if the points fall toward the diagonal line, multivariate normality is fulfilled (Kline, 2011).

As shown in Table 11, the skewness of the all the latent variables was within the required range of -1 to +1, which showed that the assumption of normality held. Also, the Q-Q plots for all the latent variables in Figure 14, in which the data points all fall very close to the ideal diagonal line, indicates normality of the data.

Table 11. Kurtosis and Skewness Test for Normality

| | Skewness | | Kurtosis | |
|---|---|---|---|---|
| | Statistic | Std. error | Statistic | Std. error |
| Performance expectancy | -0.469 | 0.194 | 0.101 | 0.385 |
| Effort expectancy | -0.352 | 0.194 | -0.199 | 0.385 |
| Social influence | -0.06 | 0.194 | -0.767 | 0.385 |
| Facilitating conditions | -0.571 | 0.194 | 0.031 | 0.385 |
| Trust | -0.599 | 0.194 | -0.001 | 0.385 |
| Security concern | -0.031 | 0.194 | 0.18 | 0.385 |
| Privacy concern | -0.276 | 0.194 | -0.742 | 0.385 |
| Perceived risk | -0.031 | 0.194 | -1.011 | 0.385 |
| Behavioral intention | -0.702 | 0.194 | 0.092 | 0.385 |

*Note*. *N* = 158.

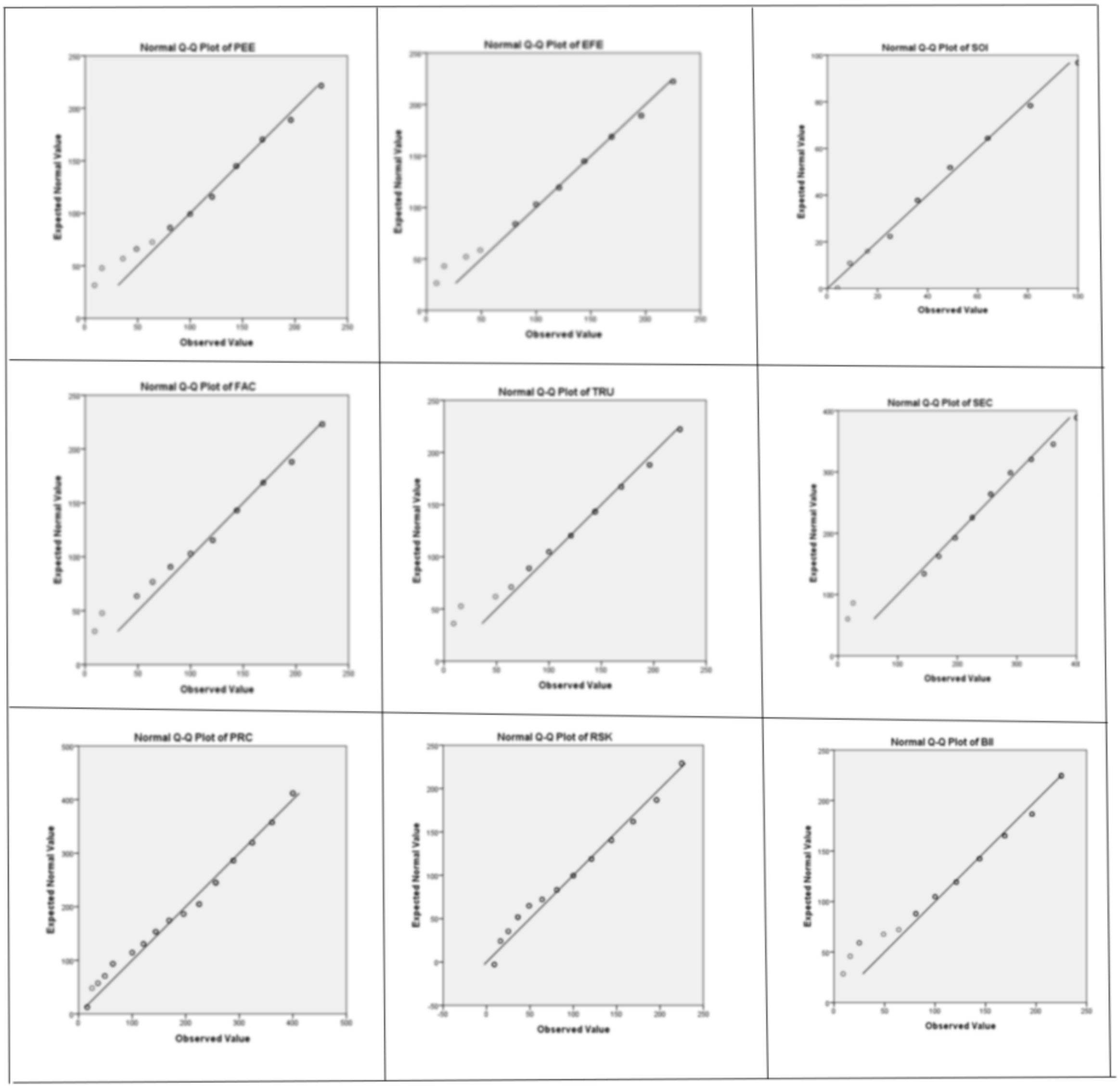


*Figure 14*. Q-Q plots for the latent variables.

### Homogeneity of Variance

Another assumption of SEM was that the level of variance for a particular variable is stabled at all levels of the predictor variable (Field, 2013). In this study, the researcher tested the assumption for homogeneity of variance using the parametric Levene’s test for equality of variances. The result of Levene’s test in Table 12 reveals that all the latent variables were nonsignificant (*p* > .001). The table shows that the variances were not significantly different; therefore, the assumption of homogeneity of variance has not been violated (Field, 2013).

Table 12. Levene’s Test for Homogeneity of Variance

| | Levene’s statistic | df1 | df2 | Sig. |
|---|---|---|---|---|
| Performance expectancy | 4.507 | 1 | 155 | .035 |
| Effort expectancy | 0.033 | 1 | 155 | .855 |
| Social influence | 0.034 | 1 | 155 | .854 |
| Facilitating conditions | 1.504 | 1 | 155 | .222 |
| Trust | 0.241 | 1 | 155 | .624 |
| Security concern | 2.747 | 1 | 155 | .099 |
| Privacy concern | 0.868 | 1 | 155 | .353 |
| Perceived risk | 0.220 | 1 | 155 | .640 |
| Behavioral intention | 0.276 | 1 | 155 | .600 |

### Multicollinearity

In the process of satisfying the assumption for multicollinearity, the assumption is that all the latent variables are independent of each other. Multicollinearity occurs when a significant correlation exists between two or more predictors in a model, which could result in higher standard errors and wider confidence intervals for coefficients. In this study, the researcher measured the multicollinearity with the variance inflation factor (VIF). The VIF is the inverse of the tolerance variable, which is the amount of variability that other predictor variables in the group cannot explain (Hair et al., 2006). As a general rule, the VIF should be less than 5 (Kock & Lynn, 2012). The result from the analysis (see Table 13) on the latent variables revealed that there was no multicollinearity issue because the largest VIF was 3.041, which is less than 5.

Table 13. Variance Inflation Factor

| | Unstandardized coefficients | | Standardized coefficients | | | Collinearity statistic | |
|---|---|---|---|---|---|---|---|
| Model | B | Std. error | Beta | *t* | Sig. | Tolerance | VIF |
| (Constant) | 21.356 | 12.067 | | 1.770 | .079 | | |
| Performance expectancy | 0.234 | 0.105 | 0.220 | 2.234 | .027 | 0.329 | 3.041 |
| Effort expectancy | 0.054 | 0.102 | 0.051 | 0.532 | .596 | 0.343 | 2.916 |
| Social influence | 0.122 | 0.157 | 0.057 | 0.778 | .438 | 0.604 | 1.654 |
| Facilitating conditions | 0.176 | 0.101 | 0.169 | 1.744 | .083 | 0.338 | 2.960 |
| Trust | 0.353 | 0.091 | 0.336 | 3.873 | .000 | 0.424 | 2.358 |
| Security concern | -0.001 | 0.059 | -0.001 | -0.010 | .992 | 0.417 | 2.398 |
| Privacy concern | -0.004 | 0.046 | -0.009 | -0.096 | .924 | 0.345 | 2.895 |
| Perceived risk | 0.034 | 0.076 | 0.043 | 0.449 | .654 | 0.355 | 2.815 |

*Note.* Dependent variable: BII.

## Measurement Model

The data analysis approach for this study centered on the two-step SEM method suggested by Anderson and Gerbing (1988). The researcher evaluated the measurement model to establish structural validity before developing the structural model for hypothesis testing. This method aimed to ensure the research model is valid, with the relationships well represented before hypothesis testing. In the two-step model, the researcher first examined the measurement model to conduct CFA and the model fit. The CFA involved examining the following: (a) reliability of the scale using Cronbach’s alpha and CR and (b) validity of the scale using convergent and discriminant validity. The researcher evaluated model fit by examining the chi-square goodness of fit test statistic, CFI, GFI, NFI, and RMSEA.

## Confirmatory Factor Analysis

Although the researcher used the validated instruments of Opala (2012) and Zhou (2012), it was pertinent to conduct a CFA to establish reliability and validity in the context of this study. The researcher assessed Cronbach's alpha and Coefficient of Reliability (CR) to demonstrate the reliability of the instrument. The Cronbach's alpha coefficients were performance expectancy (α = .831), effort expectancy (α = .826), social influence (α = .851), facilitating conditions (α = .834), trust (α = .834) and security concern (α = .820). Others were privacy concern (α = .871), perceived risk (α = .849), and behavioral intention (α = .837). All the Cronbach's alpha coefficients exceeded the minimum value of α =.70 suggested for internal consistency reliability (Field, 2013). Table 14 shows the Cronbach's alpha coefficients for individual subscales.

Table 14. Cronbach's Alpha Coefficients for Survey Subscales

| Subscale | Number of items | Cronbach's alpha |
|---|---|---|
| Performance expectancy | 3 | .831 |
| Effort expectancy | 3 | .826 |
| Social influence | 2 | .851 |
| Facilitating conditions | 3 | .834 |
| Trust | 3 | .834 |
| Security concern | 4 | .820 |
| Privacy concern | 4 | .871 |
| Perceived risk | 3 | .849 |
| Behavioral intention | 3 | .837 |

*Note*. *N* = 157.

The researcher also determined the CR coefficient, a suitable method for assessing the internal consistency of a measure. To establish internal consistency of these two research instruments, the CR should be greater than .70 (Hair, Black, Babin, & Anderson, 2010). As shown in Table 15, all the CR coefficients were higher than .70 except SOI, which was .686. However, the researcher accepted it because the Cronbach’s alpha value of SOI was very high at .851 (Nunnally, 1978; Nunnally & Bernstein, 1994).

Table 15. Estimated Factor Correlation Matrix from the Latent Variables

| | CR | AVE | MSV | MaxR(H) | PEE | EFE | SOI | SEC | RSK | TRU | BII | PRC | FAC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PEE | 0.822 | 0.607 | 0.557 | 0.823 | 0.779 | | | | | | | | |
| EFE | 0.790 | 0.558 | 0.300 | 0.899 | 0.423 | 0.747 | | | | | | | |
| SOI | 0.686 | 0.524 | 0.388 | 0.918 | | 0.286 | 0.724 | | | | | | |
| SEC | 0.737 | 0.487 | 0.377 | 0.935 | 0.143 | 0.548 | 0.551 | 0.698 | | | | | |
| RSK | 0.925 | 0.805 | 0.292 | 0.966 | -0.343 | 0.316 | 0.462 | 0.508 | 0.897 | | | | |
| TRU | 0.823 | 0.608 | 0.557 | 0.971 | 0.746 | | -0.173 | | -0.540 | 0.780 | | | |
| BII | 0.787 | 0.552 | 0.484 | 0.973 | 0.658 | 0.167 | 0.131 | 0.222 | -0.193 | 0.696 | 0.743 | | |
| PRC | 0.900 | 0.692 | 0.310 | 0.979 | 0.534 | 0.188 | -0.200 | -0.214 | | 0.557 | 0.334 | 0.832 | |
| FAC | 0.753 | 0.505 | 0.388 | 0.980 | | | 0.623 | 0.614 | 0.316 | | 0.306 | -0.334 | 0.711 |

*Note.* CR = composite reliability, AVE = average variance extracted, MSV = Maximum Shared Variance, MaxR(H) = McDonald Construct Reliability, PEE = performance expectancy, EFE = effort expectancy, SOI = social influence, FAC = facilitating conditions, TRU = trust, SEC = security concern, PRC = privacy concern, RSK = perceived risk, and BII = behavioral intention.

The researcher assessed the validity by considering the convergent and discriminant validity along with the reliability coefficients as an essential part of the CFA (Hair et al., 2010). Convergent validity is achieved when the CR value is more than the AVE, and all the AVE are statistically significant or higher than .50 (Hair et al., 2010). As indicated in Table 15, all the CR are higher than their corresponding AVE, and all the AVE meet the required minimum of .50, thereby confirming convergent validity except SEC, which had the AVE of .487, which is still within an acceptable AVE.

Discriminant validity is achieved in a situation when the measurement model is free from redundant items (Ahmad, Zulkurnain & Khairushalimi, 2016). It is the square root of individual AVE, and it should be more than any correlation between the latent variables (Zait & BERTEA, 2011). As shown in Table 15, the square root of the AVE for each construct is higher than the correlations with all other constructs and thereby demonstrated the discriminant validity of all the constructs in the study (Zait & BERTEA, 2011).

**Model Fit**

The model fit is considered for how well the model accounts for the correlations between variables in the data set (Gaskin & Lim, 2016). The researcher employed AMOS Version 24 covariance-based SEM with maximum likelihood estimation to examine the model fit and developed a measurement model to demonstrate the model fit and the various latent variables based on the theoretical model.

As shown in Figure 15, the oval shape indicates latent variables, the rectangles represent observed variables, and the circles were the error variables added to all the endogenous variables. To improve the overall model fit, the researcher modified the correlation structure between the error terms of the CFA, which resulted in covarying four error terms that were part of the same factor. Table 16 displays a goodness-of-fit test statistic. RMSEA was 0.073, which is a good fit because it is within the threshold of 0.06 (Gaskin & Lim, 2016; Hu & Bentler, 1999). The GFI was 0.815, which again reflects an acceptable good fit. The CFI was .912, which indicates an acceptable fit because it is close to the .95 threshold (Gaskin & Lim, 2016; Hu & Bentler, 1999). Also, the NFI and standardized root mean square residual were .827 and .053, respectively, which indicates an acceptable fit. Based on these baselines, an analysis of the model fit summary shows that the chi-square test was statistically significant ($\chi^2 = 519.698$, $df = 285$, $p < .001$).

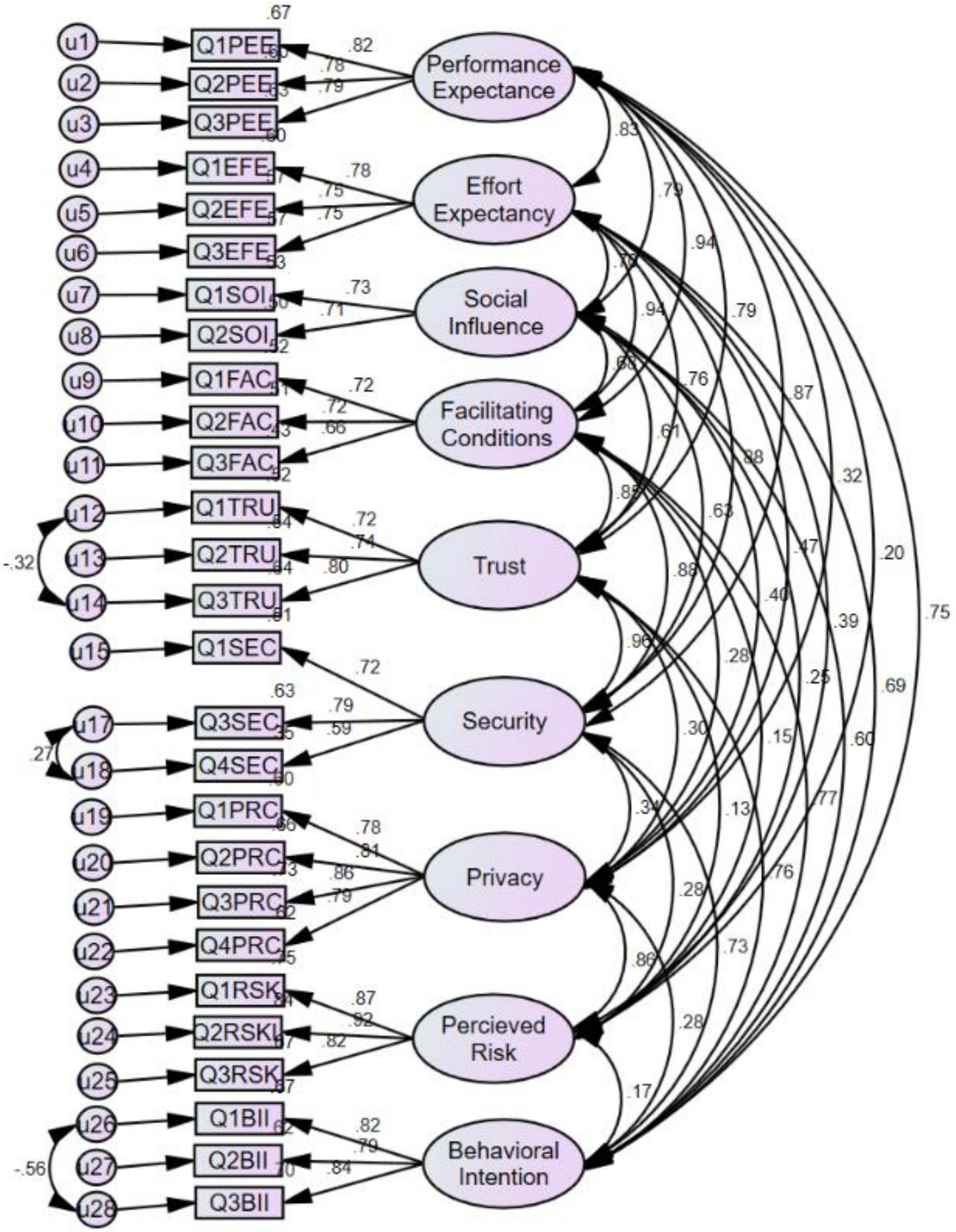


*Figure 15*. Measurement model path diagram.

Table 16. Model Fit Summary

| Model | GFI | CFI | NFI | SRMR | RMSEA |
|---|---|---|---|---|---|
| Default model | 0.815 | 0.912 | 0.827 | 0.053 | 0.073 |
| Saturated model | 1.000 | 1.000 | 1.000 | | |
| Independence model | 0.196 | 0.000 | 0.000 | | 0.220 |

*Note.* $\chi^2 = 519.698$, $df = 285$, $p < .001$. GFI = goodness-of-fit index, CFI = comparative fit index, NFI = normed fit index, SRMR = standardized root mean square, and RMSEA = mean square of approximation.

## Hypothesis Testing

The researcher tested omnibus hypothesis H1 using standard multiple regression (SMR) and hierarchical multiple regression (HMR) and tested hypotheses $H1_{01}$, $H1_{02}$, and $H1_{03}$ using structural model analysis. An explanation of the model fit precedes the results of the testing of the omnibus hypothesis. Following the results, the researcher reports a summary of the findings.

## Fit of the Model

According to Hoyt, Imel, and Chan (2008), for SMR and HMR, four values indicate the fit of the model with the data: $R$, $R^2$, $R^2_{\text{adj}}$, and the standard error of the estimate. $R$ represented the multiple correlation coefficients, and the value of $R$ can range from 0 to 1; the closer the values are to 1, the better the independent variables are in predicting the dependent variable.

## Testing of Omnibus Null Hypothesis

To test the null hypothesis, the researcher transformed the average scores for TRU, PEE, EFE, SOI, and FAC to TRU_PEE_ EFE_SOI_FAC. The researcher then totaled these variables and averaged them into one composite score labeled composite behavioral determinant in the data set. This score represented the overall or composite behavioral determinant. The composite behavioral determinant regressed against the dependent variable BII. The researcher also applied HMR analysis to test the omnibus hypothesis and to answer the omnibus research question. The omnibus hypothesis was that there was no correlation among the dimensions of trust: security, privacy, and perceived risk, UTAUT constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions), and behavioral intentions to adopt FIM.

**Result of Testing Omnibus Null Hypothesis**

The results of the HMR in Model 2 of the output indicated that the data were a good fit for the model ($R$ = .726) and that the addition of trust in the equation improved the model by 5%. As shown in Table 17, the results were significant, $F$(2,151) = 33.583, $p$ = .000 ($p$ < .01), $R^2$ = 527. The summary of the HMR model and the analysis of variance in Table 18 shows the various sums of squares and the degrees of freedom associated with each model.

Table 17. Durbin–Watson Test: Model Summary for Omnibus Hypothesis

| | | | | | Change statistics | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Model | *R* | *R* square | Adjusted *R* square | Std. error of the estimate | *R* square change | *F* change | df1 | df2 | Sig. *F* change | Durbin-Watson |
| 1 | .690[a] | .476 | .462 | 37.65373 | .476 | 34.468 | 4 | 152 | .000 | |
| 2 | .726[b] | .527 | .511 | 35.89819 | .051 | 16.230 | 1 | 151 | .000 | 2.105 |

*Note.* Dependent variable: behavioral intention.
[a]Predictors: (Constant), facilitating conditions, social influence, effort expectancy, performance expectancy.
[b]Predictors: (Constant), facilitating conditions, social influence, effort expectancy, performance expectancy, trust.

Table 18. Analysis of Variance: Sum of Squares and Degree of Freedom

| Model | | Sum of squares | *df* | Mean square | *F* | Sig. |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| | Regression | 195473.651 | 4 | 48868.413 | 34.468 | .000[a] |
| | Residual | 215506.081 | 152 | 1417.803 | | |
| | Total | 410979.733 | 156 | | | |
| 2 | | | | | | |
| | Regression | 216389.094 | 5 | 43277.819 | 33.583 | .000[b] |
| | Residual | 194590.638 | 151 | 1288.680 | | |
| | Total | 410979.733 | 156 | | | |

*Note.* Dependent variable: behavioral intention.

a Predictors: (Constant), facilitating conditions, social influence, effort expectancy, performance expectancy.
bPredictors: (Constant), facilitating conditions, social influence, effort expectancy, performance expectancy, trust.

### Testing of Null Hypotheses $H1_{01}$, $H1_{02,}$ and $H1_{03}$ Using Structural Model

Sequent to the attestation of the measurement model, the researcher connected the latent variables to represent the relationships in the hypotheses. As shown in Figure 16, the researcher replaced the covariance arrows (two-headed arrows) between the second-order constructs performance expectancy, effort expectancy, social influence, facilitating conditions, security, privacy, perceived risk, and behavioral intention with the path arrows (single-headed arrows). The SEM structural model showing the standardized regression weights and *p* values for the second order latent variables are in Table 19. The researcher analyzed the structural model to address the hypotheses and answer the research question.

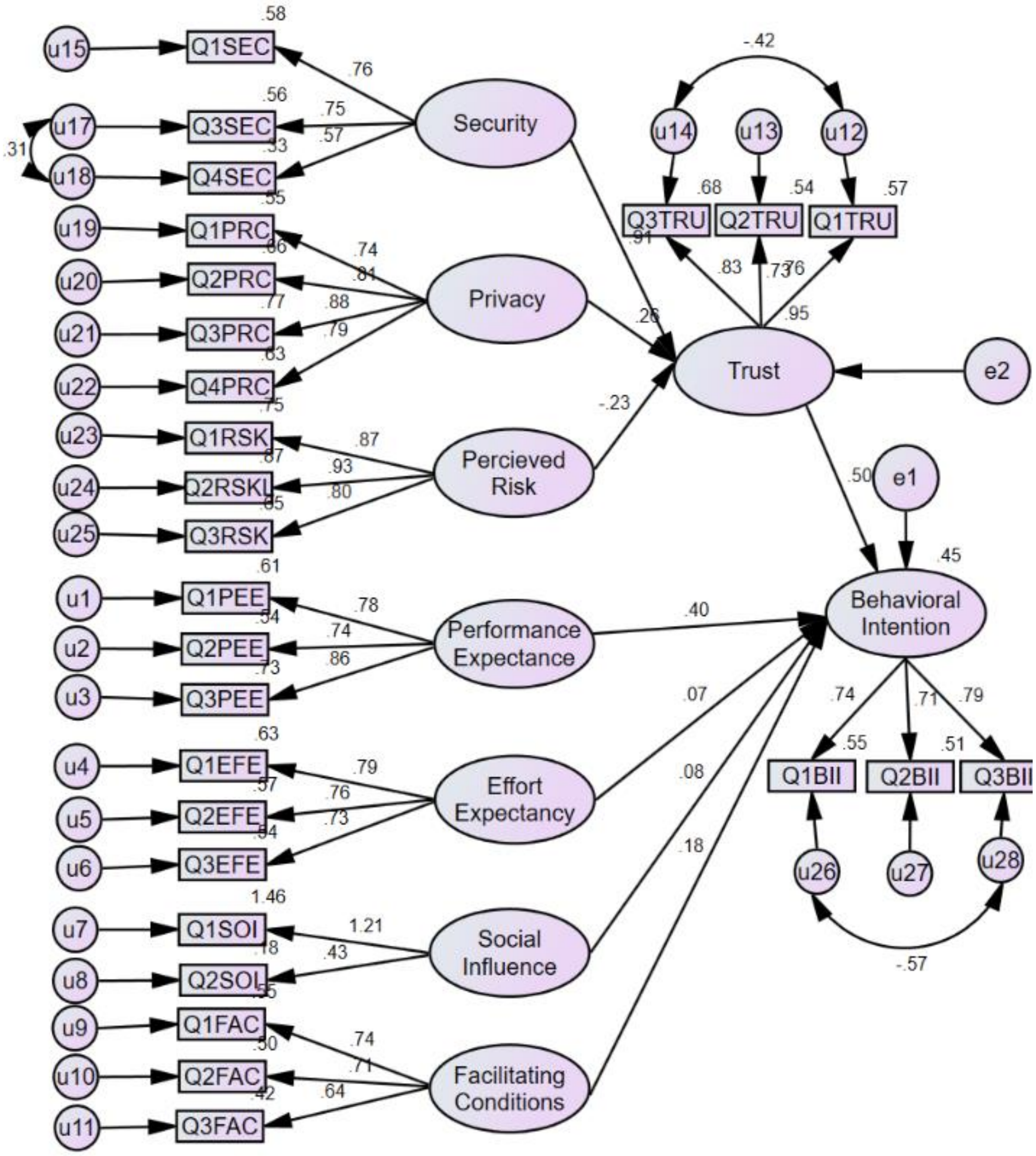


*Figure 16*. SEM structural model with standardized path coefficients

Testing Hypotheses H1$_{01}$, H1$_{02}$, and H1$_{03}$ using the SEM in Table 19 showed that security, privacy concern, and perceived risk predict trust a statistically significant level ($p$ < .001). Therefore, the researcher rejected the null hypotheses.

To obtain a discrete understanding of the contribution that each variable made to the ability of the theory to explain behavioral intention, the individual predictors underwent further examination. The researcher applied the SMR model to test the hypotheses. To examine the research question, the researcher conducted an SMR analysis to examine if trust, performance expectancy, effort expectancy, social influence, and facilitating conditions predict behavioral influence. The regression *F* test showed that the data were a good fit for the model ($R = .726$) and $F(3,151) = 33.583$, $p = .000$ ($p < .05$), $R^2 = .527$. The result showed that the overall factors had significant relationships with behavioral intention to adopt FIM.

Table 19. Summary of the Hypotheses $H1_{01}$, $H1_{02}$, and $H1_{03}$

| | | Standardized | | | *R*- | |
|---|---|---|---|---|---|---|
| Hypothesis | Path | path coefficient | *p*-value | Supported? | square | Construct |
| $H1_{01}$ | TRU ← SEC | 0.910 | *** | Yes ($p < .01$) | .95 | Trust |
| $H1_{02}$ | TRU ← PRC | 0.256 | *** | Yes ($p < .01$) | .95 | Trust |
| $H1_{03}$ | TRU ← RSK | -0.235 | *** | Yes ($p < .01$) | .95 | Trust |

*Note*. Value of *** indicates significance smaller than .001.

The researcher examined the individual predictors (see Table 20) to obtain a discrete understanding of the contribution of each variable to the ability to explain behavioral intention. The researcher observed statistical significance ($p < .05$) among all the independent variables about the dependent variable. The result of the individual predictors was that trust had the highest predictability at $p < .001$, followed by performance expectancy, which had $p < .005$.

Table 20. Results of Individual Variable Contributions

| | Unstandardized coefficients | | Standardized coefficients | | |
|---|---|---|---|---|---|
| Model | B | Std. error | Beta | *t* | Sig. |
| 2 (Constant) | 23.102 | 11.375 | | 2.031 | .044 |
| Performance expectancy | .233 | .103 | .219 | 2.263 | .025 |
| Effort expectancy | .072 | .093 | .068 | .772 | .442 |
| Social influence | .128 | .153 | .059 | .834 | .405 |
| Facilitating conditions | .170 | .099 | .164 | 1.716 | .088 |
| Trust | .347 | .086 | .330 | 4.029 | .000 |

*Note*. $F(3,151) = 33.583$, $R^2 = .527$, $p = 0.000$.

## Common Method Variance

Resulting from the suggestion by Podsakoff, MacKenzie, Lee, and Podsakoff (2003), the researcher conducted Harman's single factor test to establish if the data suffer from CMV. The Harman's single factor test is a method that is widely used by researchers to address the issue of CMV (Podsakoff et al., 2003). An indication of CMV occurs when a single factor appears from the test or when one major factor accounts for most of the covariance > 50% (Podsakoff et al., 2003). The result of Harman's single factor test in

Table 21 indicates that the significant variance explained by a single factor was 39.15%. Therefore, none of the separate variables can account for the majority of the variance. The result shows that the data are free from CMV.

Table 21. Total Variance Explained Using Harman’s Single Factor Test

| | Initial eigenvalues | | | Extraction sums of squared loadings | | |
|---|---|---|---|---|---|---|
| Component | Total | % of variance | Cumulative % | Total | % of variance | Cumulative % |
| 1 | 10.570 | 39.147 | 39.147 | 10.570 | 39.147 | 39.147 |
| 2 | 4.218 | 15.622 | 54.769 | | | |
| 3 | 1.211 | 4.485 | 59.253 | | | |
| 4 | 1.098 | 4.067 | 63.320 | | | |
| 5 | 1.031 | 3.820 | 67.140 | | | |
| 6 | .849 | 3.145 | 70.284 | | | |
| 7 | .756 | 2.800 | 73.084 | | | |
| 8 | .732 | 2.711 | 75.796 | | | |
| 9 | .650 | 2.409 | 78.204 | | | |
| 10 | .641 | 2.373 | 80.577 | | | |
| 11 | .548 | 2.031 | 82.609 | | | |
| 12 | .525 | 1.945 | 84.553 | | | |
| 13 | .477 | 1.768 | 86.322 | | | |
| 14 | .448 | 1.658 | 87.979 | | | |
| 15 | .401 | 1.487 | 89.466 | | | |
| 16 | .385 | 1.427 | 90.893 | | | |
| 17 | .350 | 1.296 | 92.188 | | | |
| 18 | .320 | 1.185 | 93.373 | | | |
| 19 | .275 | 1.018 | 94.391 | | | |
| 20 | .266 | .986 | 95.377 | | | |
| 21 | .239 | .884 | 96.261 | | | |
| 22 | .223 | .825 | 97.086 | | | |
| 23 | .202 | .749 | 97.835 | | | |
| 24 | .189 | .699 | 98.534 | | | |
| 25 | .154 | .571 | 99.105 | | | |
| 26 | .126 | .465 | 99.570 | | | |
| 27 | .116 | .430 | 100.000 | | | |

*Note.* Extraction method: Principal component analysis.

## Summary

Chapter 4 contained the results of the study. The administration of the online survey to the participants took place through Qualtrics and included 168 respondents. The researcher conducted a pre-data-screening in SPSS, which included an analysis of missing data and treatment of outliers that resulted in a final sample size of 157 participants. The researcher conducted a descriptive analysis using SPSS and met all the assumptions for SEM. As shown in Tables 17 and 19, all the hypotheses supported the theory.

# CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

## Introduction

This chapter includes the discussion, implications, and recommendations of the study beginning with a summary of the results, followed by a discussion of the results and conclusions based on the results. The chapter also includes the limitations of the study and implications for practice by considering the practical and theoretical implications of the results. Chapter 5 continues with recommendations for further research and a conclusion.

## Summary of the Results

As discussed in the introduction of Chapter 1 and literature review in Chapter 2, employees feel frustrated when they must access a myriad of organization resources over the Internet to perform their daily activities using long and complicated login credentials. The management and control of employee identity information have become a daunting task due to the complexity and fragmented nature of organizations' identity information, and the result has led to increases in behavioral intention to adopt an FIM solution. According to prior studies, the popularity of FIM is a result of the significant associated benefits, such as cost reductions in managing individual identities, and an efficient and convenient way of delivering identity services between different organizations (Arias-Cabarcos et al., 2012; Catuogno & Galdi, 2014; Lynch, 2011).

The review of the literature revealed that, despite the potential business value of adopting FIM becoming well-known within the IT community, the adoption of such technology still faces numerous challenges (Arias-Cabarcos et al., 2012). Various technology adoption researchers such as TAM (Ayhan, Comitz, & Gerberick, 2015), TOE (Bradford, Earp, & Grabski, 2014), and

UTAUT (Alotaibi & Wald, 2013; Jensen & Nyre, 2013) have applied different theories to determine user acceptance of FIM. Researchers have also considered trust as a possible inhibitor to the adoption of FIM due to employees distributing and transmitting sensitive information across various domains using loosely coupled network protocols (Maler & Reed, 2008). Numerous studies have shown trust was the biggest obstacle preventing many organization leaders from adopting FIM (Odeyinde, 2014; Satchell et al., 2011; Venkatesh et al., 2003, 2012). For example, Lee et al. (2010) revealed the critical role trust played in users' acceptance of IT.

Based on the preceding, many researchers have found that trust is the main reason consumers' attitude toward adopting this innovative technology has not been favorable. One of the significant challenges of FIM is the management of trust relationships among the federated partners and ensuring all trusted partners are living up to their promise (AlQatan et al., 2012; Buecker et al., 2008; Meng et al., 2008). To establish and maintain trust relationships, federated partners can limit federated users' activity by implementing technical and procedural solutions, monitor the security of the domain partners, and ensure the establishment of a legal agreement (Temoshok & Abruzzi, 2016).

In addition to trust, extant studies have found that Venkatesh et al. (2003) overlooked trust, security, privacy, and perceived risk in the initial UTAUT model (Im et al., 2008). Furthermore, previous studies have found significant correlations between the UTAUT constructs and behavioral intention to adopt FIM (Alkhalifah & D'Ambra, 2012; Alotaibi & Wald, 2014; Jensen & Nyre, 2013; Tadesse, 2012). However, none of these researchers considered this phenomenon among decision-makers across U.S. businesses. The focus of this study was on a population of IT decision makers across U.S. businesses and involved empirically investigating their behavioral intention to adopt FIM from the standpoint of trust, security, privacy, perceived risk, and the UTAUT constructs.

Based on the stated objectives, the researcher addressed the research question on the extent the dimensions of trust (security, privacy, and perceived risk) and UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions relate to the behavioral intentions to adopt FIM. Based on these questions, the researcher developed four hypotheses.

The target population for the study was IT decision makers across the United States who were potential adopters of FIM and were between 21 and 70 years of age. Qualtrics Audience provided the sampling frame used, and the population consisted of IT decision makers across U.S. businesses who were part of the Qualtrics Audience panel. The instruments used were location-based technology acceptance and use of technology instrument developed by Zhou (2012) and cloud adoption developed by Opala (2012), which were validated instruments that comprised an adaptation of the nine main constructs examined in this study.

One hundred sixty-eight participants responded to the survey. The researcher conducted pre-data-screening in SPSS, including an analysis of missing data and the treatment of outliers that produced a final sample size of 157 participants. The researcher conducted a descriptive analysis using SPSS and met all SEM assumptions: the sample size was large enough with no missing data or extreme outliers and assumptions of linearity, normality, homogeneity of variance, and multicollinearity.

The researcher performed CFA to identify relationships and patterns among the variables in each independent variable category. The results from the factor analysis revealed that the scores obtained were sufficient to determine the relationships of variables in each category. The researcher further conducted SMR and HMR analysis on the data to show if variables of interest explained a statistically significant amount of variance in the dependent variable.

## Discussion of the Results

To address the research question, the researcher performed a regression analysis to determine the significant relationships between the variables and the influencing of independent factors on a dependent variable.

**RQ1.** To what extent do the dimensions of trust (security, privacy, and perceived risk) relate to the behavioral intentions to adopt FIM, in conjunction with the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business?

Although the regression analysis results depict that trust, performance expectancy, effort expectancy, social influence, and facilitating conditions are strong influencing factors and have significant relationships with the behavioral intention to adopt FIM. However, the result of the individual predictors revealed that trust had the highest predictability at $p < .001$. This result was consistent with previous studies in which researchers examined trust as the highest predictor of the behavioral intention to adopt IT (Kesharwani & Singh Bisht, 2012; Lee et al., 2010; Meng et al., 2008; Ponte et al., 2015; Premarathne et al., 2017).

Esteva-Armida and Rubio-Sanchez (2014) tested the appropriateness of the UTAUT model in the context of end-user consumption. The result of the study was that trust has the highest correlation and significance with the behavioral intention to adopt a technology. Lee et al. (2010) explored the precise impact of trust and perceived risk on the core constructs of

UTAUT. The result of the study also showed high correlation and significance with the behavioral intention to adopt a technology. Shin (2010) also examined the effects of trust, security, and privacy in social networking to understand the pattern of adoption. The result established trust as a distinct construct to predict technology adoption. Meng et al.'s (2008) study on trust in mobile commerce adoption also revealed that trust and other traditional trust factors were seen as antecedents to predict technology adoption.

The analysis revealed strong statistically significant support for Hypothesis H1, which posited that trust, performance expectancy, effort expectancy, social influence, and facilitating conditions predict behavioral intention to adopt FIM at a statistically significant level. Thus, if users feel that using FIM improves their trust confidence, job performance, ease of use, and knowledge necessary, they feel more motivated to use FIM, so users who expect to gain benefits from using FIM will have a higher behavioral intention to adopt FIM. This finding is consistent with prior studies (Escobar-Rodríguez & Carvajal-Trujillo, 2014; Venkatesh et al., 2003; Zhou, 2012) and highlights a broad assertion that trust, performance expectancy, effort expectancy, social influence, and facilitating conditions are a critical factor for motivating the use of technology.

Hypothesis $H1_{01}$ posited that security concern would positively correlate with trust, which predicts behavioral intention to adopt FIM at a statistically significant level. Therefore, users will feel concerned about the security of the technology used in the FIM, which is consistent with the findings by other researchers who found security concerns as a possible inhibitor to adopt FIM (Escobar-Rodríguez & Carvajal-Trujillo, 2014; Tadesse, 2012). It further corroborated Jensen and Jaatun's (2013) conclusion that the most prominent concern faced in adopting FIM in many organizations was that an unauthorized user could get access to, and control, their production process and would increase the enterprise systems' attack surface. The fear was that someone could authenticate as another user and then automatically get access to all the companies where this user has access rights (Jensen & Jaatun, 2013).

Hypothesis $H1_{02}$ posited that privacy concern would positively correlate with trust, which predicts behavioral intention to adopt FIM at a statistically significant level. The hypothesis indicates that if FIM providers can provide the level of assurance that users' personal information will be appropriately collected, transmitted securely, stored, and used, the trust level of the users will improve and behavioral intention to adopt FIM will increase in turn. The result of this hypothesis was in line with the findings by other researchers who found privacy concerns to be a possible inhibitor to adopting FIM (Escobar-Rodríguez & Carvajal-Trujillo, 2014; Odeyinde, 2014; Zhou, 2012).

Hypothesis $H1_{03}$ posited that perceived risk would positively correlate with trust, which predicts behavioral intention to adopt FIM at a statistically significant level. The hypothesis indicated the likelihood of unfavorable outcomes and consequences resulting from unauthorized access to organizations' sensitive data. The result of this hypothesis was in line with the findings of other researchers who found perceived risk as a possible inhibitor of behavioral intention to adopt FIM (Odeyinde, 2014; Zhou, 2012).

## Conclusions Based on the Results

Analysis of the regression analysis results revealed that trust, performance expectancy, effort expectancy, social influence, and facilitating conditions are strong influencing factors and have significant relationships with the behavioral intention to adopt FIM. The study further showed that trust has the highest correlation and significance with the behavioral intention to adopt a technology. The study also revealed that security, privacy concern, and perceived risk predict trust at a statistically significant level, which in turn predicts behavioral intention to adopt FIM.

## Limitations

Several limitations in this study require further examination and additional research. First, the focus of this study was on respondents with experience making IT decisions for organizations and did not involve considering individual experience using FIM. Karahanna, Straub, and Chervany (1999) suggested that the basis of the determinants of behavioral intention should be user level of experience.

Second, the attitude, personality, and value of the top management play a critical role in the organizational decision-making process. Several studies revealed that the top management's role in any organization is decisive, as the decisions may affect the current and future activities of the company positively or negatively (Amaio, 2009; Chaudhry et al., 2012; Shang & Lin, 2010). Researchers had not articulated or tested the linkages between top management actions and behavior intention to adopt technology in much of the empirical literature. Researchers had also not considered the direct impact of these leadership traits on behavioral intention to adopt FIM.

Third, even though the FIM offers economic benefit to organizations, researchers had not considered the perceived value to the organization of adopting the technology. Perceived value is defined "as the consumer's overall assessment of the utility of a product or service based on perceptions of" who receives, gives, or trades off (Morar, 2013; Zeithaml, 1988, p. 14). The customers of a product or service place value based on the product’s technical ability to fulfill a need and provide satisfaction (Zeithaml, 1988). Researchers have revealed a positive correlation between perceived value and behavioral intentions (Chen, 2008; Chen & Chen, 2010; Hsu & Lin, 2015; Pandža Bajs, 2015).

Another possible limitation was that security, privacy, and perceived risk could have a direct effect on predicting behavioral intentions to adopt FIM. Even though several researchers have conducted studies on individual factors, none of these studies have considered the direct consequence of these constructs on the behavioral intention to adopt innovative technology. Finally, Fowler (2009) noted voluntary studies have a potential bias, as potential participants may be unwilling or unable to participate in the survey.

## Implications for Practice

Understanding the correlation between the dimensions of trust (privacy, security, and perceived risk), the UTAUT constructs, and behavioral intention to adopt FIM as addressed in this study has significant theoretical and practical implications. The first theoretical implication was that this research contributed to the body of knowledge on the adoption of FIM by IT decision maker. The results of the research can provide scholars a foundation for further studies using, for example, the extensions of UTAUT2 to provide a deeper understanding of the phenomenon. The study provides information on the correlation between the dimension of trust (security, privacy, and perceived risk) in conjunction with the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions in U.S. business to adopt FIM. Researchers can use this study as a reference point for future studies in this context.

This research could contribute to the study of IT concerning the UTAUT, even though there is skepticism among organization executives in accepting FIM due to concerns of trust (AlQatan et al., 2012) and experts from the various fields of study have viewed trust with diverse viewpoints. This study could provide organizational leaders with a clearer perspective of the trust factors associated with adoption of FIM.

In addition, this study provides empirical evidence on trust, and the UTAUT construct behavioral intention to adopt FIM, so organizational leaders can leverage the results from this study to understand what influence that contributes to IT decision maker to adopt new technologies in general, and especially the trust factors that influence the adoption of FIM. It will help the organizations in defining policies and practices that allow businesses to maximize the benefits of FIM to their organization.

## Recommendations for Further Research

Future research should include IT decision makers with experience using FIM. Future researchers should consider the direct effects of leadership traits (attitude, personality, and value) on behavioral intention to adopt FIM. Future researchers should also investigate the linkages between top management actions and behavioral intention to adopt a technology. Even though FIM offers economic benefit to organizations, researchers have not considered the perceived value to organizations of adopting the technology. The introduction of innovative technology to an organization may offer an economic advantage, but a perceived value of the technology that is not commensurate for small and medium-size organizations may inhibit the behavioral intention to adopt such technology. Future researchers should investigate the effect of perceived risk on the behavioral intention to adopt FIM. Based on the new UTAUT, the items related to security, privacy, and perceived risk would have a direct effect on behavioral intentions to adopt FIM. Future researchers should also consider the effect of these constructs on consumers' behavioral intention.

## Conclusion

The goal of this research was to contribute to knowledge about the predictors of FIM in the context of technology adoption. FIM has become a necessary technology that creates global interoperable identities. Its use implies that organizations can participate through federating their identity through common, shared authentication processes and access multiple online organizations and services (Temoshok, 2016). Drawing on the UTUAT model of Venkatesh et al. (2003, 2012), the researcher investigated the extent to which trust and UTAUT constructs relate to the behavioral intentions to adopt FIM in U.S. business.

The study included a correlational design to address the research question and IT decision makers completed a survey questionnaire to measure their perceptions of trust, performance, effort expectancy, social influence, and facilitating conditions on the behavioral intention to adopt FIM. The findings from the survey revealed that trust, performance expectancy, effort expectancy, social influence, and facilitating condition together predicted behavioral intention to adopt FIM at a statistically significant level. Moreover, the findings also showed that trust was the most reliable predictor of behavioral intention to adopt FIM. In conclusion, the findings of the research provide support to the effectiveness of the UTAUT framework for advancing insight into trust as a predictor of behavioral intention to adopt FIM.

# REFERENCES

Ahmad Khattak, Z., Ab Manan, J., & Sulaiman, S. (2012). Trustworthy mutual attestation protocol for local true single sign-on system: Proof of concept and performance evaluation. *Transactions on Internet and Information Systems (Seoul), 6*(9), 2405–2423. doi:10.3837/tiis.2012.09.025

Ahmad, S., Zulkurnain, N. N. A., & Khairushalimi, F. I. (2016). Assessing the validity and reliability of a measurement model in structural equation modeling (SEM). *British Journal of Mathematics & Computer Science 15*(3): 1-8. doi:10.9734/BJMCS/2016/25183

Ahmadi, H., Nilashi, M., & Ibrahim, O. (2015). Organizational decision to adopt hospital information system: An empirical investigation in the case of Malaysian public hospitals. *International Journal of Medical Informatics, 84*(3), 166-188. doi:10.1016/j.ijmedinf.2014.12.004

Ahn, G. J. (2016). *U.S. Patent No. 9,338,188*. Washington, DC: U.S. Patent and Trademark Office. Retrieved from https://patents.google.com/patent/US9338188B1/en

Ajzen, I. (1985). From intentions to actions: A theory of planned behaviour. In J. Kuhl & J. Beckman (Eds.), *Action-control: From cognition to behaviour* (pp. 11–39). Heidelberg, Germany: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections. *Psychology and Health 26(9),* 1113–1127. doi:10.1080/08870446.2011.613995

Ajzen, I., & Fishbein, M. (1969). The prediction of behavioral intentions in a choice situation. *Journal of Experimental Social Psychology, 5*(4), 400–416. doi:10.1016/0022-1031(69)90033-X

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior.* Englewood Cliffs, NJ: Prentice-Hall, Inc.

Alkhalifah, A., & D'Ambra, J. (2015, May). *Identity Management Systems Research: Frameworks, Emergence, and Future Opportunities. In 23rd European Conference on Information Systems* (pp. 1-16). ECIS. Retrieved from http://aisel.aisnet.org/ecis2015_cr/6/

Alkhalifah, A., & Amro, A. (2017). Understanding the effect of privacy concerns on user adoption of identity management systems. *Journal of Computers, 12*(2), 174–182. doi:10.17706/jcp.12.2

Alkhalifah, A., & D'Ambra, J. (2012). Factors affecting user adoption of identity management systems: An empirical study. In *Proceedings of the 2012 Pacific Asia Conference on Information Systems (PACIS)* (pp. 182-194). Association for Information Systems AIS Electronic Library (AISeL). Retrieved from https://aisel.aisnet.org/pacis2012/182

Al-Mamary, Y. H., Al-nashmi, M., Hassan, Y. A. G., & Shamsuddin, A. (2016). A Critical Review of Models and Theories in Field of Individual Acceptance of Technology. *International Journal of Hybrid Information Technology, 9*(6), 143-158. doi:10.14257/ijhit.2016.9.6.13

Alotaibi, S. J., & Wald, M. (2013, December). Evaluation of the UTAUT model for acceptable user experiences in identity access management systems. In *8th International Conference for Internet Technology and Secured Transactions* (pp. 232-237). IEEE. doi:10.1109/ICITST.2013.6750197

Alotaibi, S. J., & Wald, M. (2014). Discussion and evaluation of the updated UTAUT model in IAMS. *International Journal of Intelligent Computing Research*, *5*(1/2), 1–10. Retrieved from http://eprints.soton.ac.uk/id/eprint/363442

Alpár, G., Hoepman, J. H., & Siljee, J. (2011). The identity crisis. Security, privacy and usability issues in identity management. Scientific Publication. Retrieved from http://arxiv.org/ftp/arxiv/papers/1101/1101.0427.pdf.

AlQatan, S., Singh, D., & Ahmad, K. (2012). Study on success factors to enhance customer trust for mobile commerce in small and medium-sized tourism enterprises (SMTEs): A conceptual model. *Journal of Theoretical and Applied Information Technology, 46(2),* 550–564. Retrieved from http://www.jatit.org/volumes/Vol83No3/8Vol83No3.pdf

Amaio, T. E. (2009). *Exploring and examining the business value of information security: Corporate executives' perceptions* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3351834)

American Institute of Certified Public Accountants. (2011). AICPA/CICA privacy maturity model. Retrieved from http://www.cil.cnrs.fr/CIL/IMG/pdf/10-229_aicpa_cica_privacy_maturity_model_finalebook_revised.pdf

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411. doi:10.1037/0033-2909.103.3.411

Anderson, M. (2015). Technology device ownership: 2015. Retrieved from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015

Angeles, R. (2014). Using the technology-organization-environment framework for analyzing Nike's "considered index" green initiative, a decision. *Journal of Management and Sustainability, 4*(1), 96–113. doi:10.5539/jms.v4n1p96

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. Management *Information Systems Quarterly, 33*(2), 339–370. doi:10.2307/20650295

Arias-Cabarcos, P., Almenárez-Mendoza, F., Marín-López, A., Díaz-Sánchez, D., & Sánchez-Guerrero, R. (2012). A metric-based approach to assess risk for ‘on cloud’ federated identity management. *Journal of Network and Systems Management, 20*(4), 513–533. doi:10.1007/s10922-012-9244-2

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the “bring your own device” paradigm. *Computer, 47*(6), 48–56. doi:10.1109/MC.2014.164

Awa, H. O., Ukoha, O., & Emecheta, B. C. (2016). Using TOE theoretical framework to study the adoption of ERP solution. *Cogent Business & Management, 3*(1), 1-23. doi:10.1080/23311975.2016.1196571

Ayed, G. B., & Ghernaouti-Hélie, S. (2012, August). *Processes view modeling of identity-related privacy business interoperability: considering user-supremacy federated identity technical model and identity contract negotiation*. In Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on (pp. 906-913). IEEE. doi.10.1109/ASONAM.2012.162

Ayhan, S., Comitz, P., & Gerberick, G. (2015, April 21–23). *Federated multi-agency credentialing*. Paper presented at the Integrated Communication, Navigation, and Surveillance Conference (ICNS). IEEE Xplore Digital Library. doi:10.1109/ICNSURV.2015.7121250

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 243–255. Retrieved from http://aisel.aisnet.org/jais/vol8/iss4/3

Baker, J. (2012). The technology–organization–environment framework, in information systems theory. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information systems theory*: *Explaining and predicting our digital society* (pp. 231–245). New York, NY: Springer Science & Business Media.

Bauman, A. E., Reis, R. S., Sallis, J. F., Wells, J. C., Loos, R. J., & Martin, B. W. (2012). Correlates of physical activity: Why are some people physically active and others not? *Lancet, 380*(9838), 258–271. doi:10.1016/S0140-6736(12)60735-1.

Bell, E., & Bryman, A. (2007). The ethics of management research: An exploratory content analysis. *British Journal of Management, 18*(1), 63–77. doi:10.1111/j.1467-8551.2006.00487.x

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems, 8*(4), 211–218. Retrieved from http://aisel.aisnet.org/jais/vol8/iss4/7

Bentler, P. M., & Chou, C. P. (1987). Practical issues in structural modeling. *Sociological Methods & Research, 16*(1), 78–117. doi:10.1177/0049124187016001004

Bertino, E., & Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. Norwood, MA: Artech House.

Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2009). Standards for web services security. In *Security for Web Services and Service-Oriented Architectures* (pp. 45-77). Springer, Berlin, Heidelberg.

Birrell, E., & Schneider, F. B. (2013). Federated identity management systems: A privacy-based characterization. *IEEE Security and Privacy, 11*(5), 36–48. doi:10.1109/MSP.2013.114

Bodnar, L. M., Westphall, C. M., Werner, J., & Westphall, C. B. (2016, February). Towards privacy in identity management dynamic federations. In *The Fifteenth International Conference on Networks, 52*, 1-45. (ISBN:978-1-61208-450-3, PMid:26753012, PMCid:PMC4706695)

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM, 58*(7), 78–87. doi:10.1145/2699390

Boomsma, A. (1985). Nonconvergence, improper solutions, and starting values in LISREL maximum likelihood estimation. *Psychometrika, 50*, 229–242. doi:10.1007/BF02294248

Boomsma, A., & Hoogland, J. J. (2001). The robustness of LISREL modeling revisited. Structural equation models: Present and future. *A Festschrift in honor of Karl Jöreskog, 2*(3), 139-168. Retrieved from https://core.ac.uk/download/pdf/20770852.pdf

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems, 15*(2), 149–165. doi:10.1016/j.accinf.2014.01.003

Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S., & Readshaw, N. (2008). *Understanding SOA security design and implementation*. Poughkeepsie, NY: IBM Redbooks.

Cabarcos, P. A., Almenárez, F., Mármol, F. G., & Marín, A. (2014). To federate or not to federate: A reputation-based mechanism to dynamize cooperation in identity management. *Wireless Personal Communications, 75*(3), 1769–1786. doi:10.1007/s11277-013-1338-y

Cao, Q., Jones, D. R., & Sheng, H. (2014). Contained nomadic information environments: Technology, organization, and environment influences on adoption of hospital RFID patient tracking. *Information & Management*, *51*(2), 225–239. doi:10.1016/j.im.2013.11.007

Cao, Y., & Yang, L. (2010, December). *A survey of identity management technology*. In Information Theory and Information Security (ICITIS), 2010 IEEE international conference on (pp. 287-293). IEEE. doi.10.1109/ICITIS.2010.5689468

Carr, L. T. (1994). The strengths and weaknesses of quantitative and qualitative research: What method for nursing? *Journal of Advanced Nursing*, *20*(4), 716–721. doi:10.1046/j.1365-2648.1994.20040716.x

Cassell, E. J. (2000). The principles of the Belmont report revisited. How have respect for persons, beneficence, and justice been applied to clinical medicine? *The Hastings Center Report*, *30*(4), 12–21. doi:10.2307/3527640

Catuogno, L., & Galdi, C. (2014). Achieving interoperability between federated identity management systems: A case of study. *Journal of High-Speed Networks*, *20*(4), 209–221. doi:10.3233/JHS-140499

Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., & Germonville, D. (2014). Adding federated identity management to OpenStack. *Journal of Grid Computing*, *12*(1), 3–27. doi:10.1007/s10723-013-9283-2

Chaudhry, P. E., Chaudhry, S., & Reese, R. (2012). Developing a model for enterprise information systems security. *Economics, Management, and Financial Markets*, *7*, 587–599. (ISSN 1842-3191)

Chen, C. F. (2008). Investigating structural relationships between service quality, perceived value, satisfaction, and behavioral intentions for air passengers: Evidence from Taiwan. *Transportation Research Part A, Policy and Practice*, *42*(4), 709–717. doi:10.1016/j.tra.2008.01.007

Chen, C. F., & Chen, F. S. (2010). Experience quality, perceived value, satisfaction and behavioral intentions for heritage tourists. *Tourism Management*, *31*(1), 29–35. doi:10.1016/j.tourman.2009.02.008

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295(2)*, 295–336. Retrieved from https://www.researchgate.net/profile/Wynne_Chin/publication/232569511_The_Partial_Least_Squares_Approach_to_Structural_Equation_Modeling/links/0deec533e0f7c00f59000000.pdf

Chung, J. E., Park, N., Wang, H., Fulk, J., & McLaughlin, M. (2010). Age differences in perceptions of online community participation among non-users: An extension of the technology acceptance model. *Computers in Human Behavior*, *26*(6), 1674–1684. doi:10.1016/j.chb.2010.06.016

Chuttur, M. Y. (2009). Overview of the technology acceptance model: Origins, developments and future directions. *Working Papers on Information Systems, 9*(37), 9-37. ISSN 1535-6078. Retrieved from http://sprouts.aisnet.org/9-37

Claudy, M., Garcia, R., & O'Driscoll, A. (2015). Consumer resistance to innovation a behavioral reasoning perspective. *Journal of the Academy of Marketing Science*, *43*(4), 528–544. doi:10.1007/s11747-014-0399-0

Cooper, D. R., & Schindler, P. S. (2011). *Qualitative research. Business research methods*, I60-182 New York: McGrew-Hill Companies.

Corazao, C. E. (2014). *Assessing factors affecting physician's intention to adopt biometric authentication technology in electronic medical records* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3579650)

Creswell, J. (2009). *Research design: Qualitative*, *quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons, 59*(6), 605-614. doi.10.1016/j.bushor.2016.08.002

Dahl, E., Tagler, M. J., & Hohman, Z. P. (2017). Gambling and the reasoned action model: Predicting past behavior, intentions, and future behavior. *Journal of Gambling Studies, Springer 33*(5), 1–18. (PMID:28623608). doi:10.1007/s10899-017-9702-6

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003. doi:10.1287/mnsc.35.8.982

Devaraj, S., Ow, T., & Kohli, R. (2013). Examining the impact of information technology and patient flow on healthcare performance: A theory of swift and even flow (TSEF) perspective. *Journal of Operations Management*, *31*(4), 181–192. doi:10.1016/j.jom.2013.03.001

De Vaus, D., Gray, M., Qu, L., & Stanton, D. (2010). *The effect of relationship breakdown on income and social exclusion: Social security, poverty and social exclusion in rich and poorer countries.* Antwerp, Brussels: Intersentia.

Dippel, E. A., Hanson, J. D., McMahon, T. R., Griese, E. R., & Kenyon, D. B. (2017). Applying the theory of reasoned action to understanding teen pregnancy with American Indian communities. *Maternal and Child Health Journal, 21*(7), 1449-1456. doi:10.1007/s10995-017-2262-7

Escobar-Rodríguez, T., & Carvajal-Trujillo, E. (2014). Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. *Tourism Management, 43*, 70–88. doi:10.1016/j.tourman.2014.01.017

Esteva-Armida, E., & Rubio-Sanchez, A. (2014). The influence of trust in the UTAUT model. In H. Nemati (Ed.), *Analyzing security, trust, and crime in the digital world* (pp. 162–186). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-4856-2.ch008

Fair Credit Reporting Act 15 U.S.C § 1681 (2012). Retrieved from https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160. doi:10.3758/BRM.41.4.1149

FedRAMP (2017). Make the Most of the FedRAMP Marketplace. Retrieved from https://www.fedramp.gov/make-the-most-of-the-fedramp-marketplace/

Fett, D., Küsters, R., & Schmitz, G. (2017). *The web SSO Standard OpenID Connect: In-depth formal security analysis and security guidelines*. doi:10.1109/CSF.2017.20

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Thousand Oaks, CA: Sage.

Fogarty, G. J., & Shaw, A. (2010). Safety climate and the theory of planned behavior: Towards the prediction of unsafe behavior. *Accident: Analysis and Prevention, 42*(5), 1455–1459. doi:10.1016/j.aap.2009.08.008

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160. doi:10.1016/j.chb.2008.08.006

Fowler, F. J. (2009). *Survey research methods* (4th ed.). Thousand Oaks, CA: Sage. doi:10.4135/9781452230184

Gabriele, E. F. (2003). The Belmont ethos: the meaning of the Belmont Principles for human subject protections. *Journal of Research Administration, 34*(2), 19. Retrieved from https://www.questia.com/library/journal/1P3-743664091/the-belmont-ethos-the-meaning-of-the-belmont-principles

Gangopadhyay, K., Nishimura, A., & Pal, R. (2016). Can the information technology revolution explain the incidence of co-movement of skill premium and stock prices?. Economic Modelling, 53, 107-120. doi.10.1016/j.econmod.2015.11.003

Gaskin, J., & Lim, J. (2016). *Master validity tool: AMOS plugin.* Gaskination's StatWiki. Retrieved from http://statwiki.kolobkreations.com/index.php?title=Main_Page

General Services Administration. (2012). Federal risk and authorization management program (FedRAMP). Retrieved from http://csrc.nist.gov/groups/SMA/forum/documents/FedRAMP-Goodrich-020912.pdf

Ghazizadeh, E., Zamani, M., Ab Manan, J., & Pashang, A. (2012, December). *A survey on security issues of federated identity in the cloud computing.* In *4th International Conference on Cloud Computing Technology and Science* (pp. 532–565). doi:10.1109/CloudCom.2012.6427513

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Identity Guidelines*. (No. Special Publication (NIST SP-800-63). doi:10.6028/NIST.SP.800-63-3

Grassi, P., Lefkovitz, N., & Mangold, K. (2015). *Privacy-Enhanced Identity Brokers*. NIST-NCCoE.

Ha, H. Y., & Janda, S. (2017). Predicting consumer intentions to purchase energy-efficient products. In C. L. Campbell (Ed.), *The customer is not always right? Marketing orientations in a dynamic business world* (pp. 897-897). New York, NY: Springer. doi:10.1007/978-3-319-50008-9_249

Hackett, M., & Hawkey, K. (2012). *Security, privacy and usability requirements for federated identity*. In Workshop on Web (Vol. 2). Retrieved from http://w2spconf.com/2012/papers/w2sp12-final18.pdf

Haghshenas, A., & Seyyedi, M. (2012). Federated identification architecture. *International Journal of Computer Applications, 52*(16), 0975–8887. Retrieved from https://pdfs.semanticscholar.org/1900/65bed632e0769951c12215b14dd56a7f0d78.pdf

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice-Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (6th ed.). Upper Saddle River, NJ: Pearson.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). *An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the academy of marketing science, 40*(3), 414-433. doi:0.1007/s11747-011-0261-6

Halpin, H., & Cook, B. (2012, October). Federated identity as capabilities. In *proceeding of 2012 Annual Privacy Forum*, 125-139. doi:10.1007/978-3-642-54069-1

Han, J., Mu, Y., Susilo, W., & Yan, J. (2010, September). A generic construction of dynamic single sign-on with strong security. In *International Conference on Security and Privacy in Communication Systems* (pp. 181-198). Springer, Berlin, Heidelberg.

Hardt, D. (2012). The OAuth 2.0 authorization framework. Retrieved from https://tools.ietf.org/html/rfc6749

Haumont, D., NguyenBa, C., & Modi, N. (2017). eNewborn: The Information Technology Revolution and Challenges for Neonatal Networks. *Neonatology, 111*(4), 388-397. doi.org/10.1159/000464267

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing, 18*(3), 66-67. doi:10.1136/eb-2015-102129

Hoellrigl, T., Dinger, J., & Hartenstein, H. (2010, July). A consistency model for identity information in distributed systems. In *Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual* (pp. 252-261). IEEE.

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: Its past and its future in health care. *Journal of Biomedical Informatics, 43*(1), 159–172. doi:10.1016/j.jbi.2009.07.002

Hox, J. J., & Bechger, T. M. (1998). An introduction to structural equation modeling. *Family Science Review, 11*, 354-373. Retrieved from http://joophox.net/publist/semfamre.pdf

Hoyle, R. H. (Ed.). (1999). *Statistical strategies for small sample research.* Thousand Oaks, CA: Sage.

Hoyt, W. T., Imel, Z. E., & Chan, F. (2008). Multiple regression and correlation techniques: Recent controversies and best practices. *Rehabilitation Psychology, 53*(3), 321-339. doi:10.1037/a0013021

Hsu, C. L., & Lin, J. C. C. (2015). What drives purchase intention for paid mobile apps? An expectation confirmation model with perceived value. *Electronic Commerce Research and Applications, 14*(1), 46–57. doi:10.1016/j.elerap.2014.11.003

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. doi:10.1080/10705519909540118

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2) 195–204. doi:10.1002/(SICI)1097-0266(199902)20:23.0.CO;2-7

Im, I., Kim, Y., & Han, H. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & Management, 45*(1), 1–9. doi:10.1016/j.im.2007.03.005

Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, *93*(1), 7–28. doi:10.1016/j.jretai.2016.12.006

Isaakidis, M., Halpin, H., & Danezis, G. (2016, October). UnlimitID: Privacy-preserving federated identity management using algebraic MACs. *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (pp. 139–142). doi:10.1145/2994620.2994637

International Standard Organization. (2011).  A framework for identity management - Part 1: Terminology and concepts. ISO/IEC 24760-1:2011. Retrieved from https://www.iso.org/standard/57914.html

Jensen, J. (2011). Benefits of federated identity management: A survey from an integrated operations viewpoint. Availability, Reliability and Security for Business, Enterprise and Health Information Systems, 1–12. doi:10.1007/978-3-642-23300-5_1

Jensen, J. (2012, August). Federated identity management challenges. In *Seventh International Conference on Availability, Reliability and Security* (pp. 230–235). IEEE. doi:10.1109/ARES.2012.68

Jensen, J., & Jaatun, M. G. (2013). Federated identity management—We built it; why won't they come? *IEEE Security and Privacy, 11*(2), 34–41. doi:10.1109/MSP.2012.135

Jensen, J., & Nyre, A. A. (2013, September). Federated identity management and usage control-obstacles to industry adoption. In *Eighth International Conference on Availability, Reliability and Security* (pp. 31–41). doi:10.1109/ARES.2013.10

Jirotka, M., Lee, C. P., & Olson, G. M. (2013). Supporting scientific collaboration: Methods, tools and concepts. *Computer Supported Cooperative Work, 22*(4-6), 667–715. doi:10.1007/s10606-012-9184-0

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *Management Information Systems Quarterly, 23*(2), 183–213. doi:10.2307/249751

Kaspersky Lab. (2015). Phishing attack list: Windows Live ID scam. *MIT's IT Security Information Newsletter*. Retrieved from https://securityfyi.wordpress.com/2015/05/28/phishing-attack-list-windows-live-id-scam/

Katalov, V. (2015). How Secure Is Your Password? A Friendly Advice from a Company That Breaks Passwords. *Forensic Focus*.  Retrieved from https://articles.forensicfocus.com/2015/02/01/how-secure-is-your-password-a-friendly-advice-from-a-company-that-breaks-passwords/

Kenny, G. (2016). *'To protect my health, or to protect my health data?' Examining the influence of health information privacy concerns on citizens' health technology adoption* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 21385)

Kesharwani, A., & Singh Bisht, S. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing, 30*(4), 303–322. doi:10.1108/02652321211236923

Khara, S., & Gupta, A. (2017). Security issues in cloud. *International Journal of Innovations & Advancement in Computer Science, 6*(1), 8–12. ISSN 2347–8616. Retrieved from http://www.academicscience.co.in/admin/resources/project/paper/f201701061483723464.pdf

Kim, Y. J. (2009). Access control service oriented architecture security. Washington University in St. Louis, Student Reports project on Recent Advances in Network Security. Retrieved from http://www.cse.wustl.edu/~jain/cse571-09/ftp/soa/index.html#sec2.1

Kleijnen, M., Lee, N., & Wetzels, M. (2009). An exploration of consumer resistance to innovation and its antecedents. *Journal of Economic Psychology*, *30*(3), 344–357. doi:10.1016/j.joep.2009.02.004

Kleis, L., Chwelos, P., Ramirez, R., & Cockburn, L. (2012). Information technology and intangible output: The impact of IT investment on innovation productivity. *Information Systems Research, 23(1)*, 42–59. doi:10.1287/isre.1100.0338

Kline, R. B. (2005). *Methodology in the social sciences. Principles and practice of structural equation modeling, 2nd ed*. New York: Guilford Press

Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling* (5th ed., pp. 3–427). New York: The Guilford Press.

Ko, M. N., Cheek, G. P., Shehab, M., & Sandhu, R. (2010). Social-networks connect services. *Computer, 43*(8), 37–43. doi:10.1109/MC.2010.239

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546–580. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152644

Kuan, K. K., & Chau, P. Y. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & management, 38*(8), 507-521. doi.org/10.1016/S0378-7206(01)00073-8

Kurowski, S. (2015). *Economic issues of federated identity management-an estimation of the costs of identity lifecycle management in inter-organizational information exchange* *using transaction cost theory*. Open Identity Summit 2015. Retrieved from http://subs.emis.de/LNI/Proceedings/Proceedings251/85.pdf

Lai, W. T., & Chen, C. F. (2011). Behavioral intentions of public transit passengers: The roles of service quality, perceived value, satisfaction and involvement. *Transport Policy, 18*(2), 318–325. doi:10.1016/j.tranpol.2010.09.003

Lee, T. (2005). The impact of perceptions of interactivity on customer trust and transaction intentions in mobile commerce. *Journal of Electronic Commerce Research, 6*(3), 165. Retrieved from http://www.jecr.org/sites/default/files/06_3_p01.pdf

Lee, J., Kim, S., & Song, C. (2010). The effects of trust and perceived risk on users' acceptance of ICT services. doi:10.2139/ssrn.1703213

Lee, Y. H., Hsieh, Y. C., & Hsu, C. N. (2011). Adding innovation diffusion theory to the technology acceptance model: Supporting employees' intentions to use e-learning systems. *Journal of Educational Technology & Society, 14*(4), 124–137. Retrieved from http://www.jstor.org/stable/jeductechsoci.14.4.124

Li, W., & Mitchell, C. J. (2016). Analysing the Security of Google's implementation of OpenID Connect. In *Detection of intrusions and malware, and vulnerability assessment* (pp. 357–376). Springer International Publishing, doi:10.1007/978-3-319-40667-1_18

Lo, J. (2010). Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites. *AMCIS 2010 Proceedings*. Paper 110. Retrieved from http://aisel.aisnet.org/amcis2010/110/

Lynch, L. (2011). Inside the identity management game. *IEEE Internet Computing, 15*(5), 78–82. doi:10.1109/MIC.2011.119

Maler, E., & Reed, D. (2008). The Venn of identity: Options and issues in federated identity management. *IEEE Security and Privacy, 6*(2), 16–23. doi:10.1109/MSP.2008.50

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. doi:10.1287/isre.1040.0032

Marsh, H. W., & Hau, K. T. (1999). Confirmatory factor analysis: Strategies for small sample sizes. In R. H. Hoyle (Ed.), *Statistical Strategies for Small Sample Size* (pp. 251–284). Thousand Oaks, CA: Sage

Masoud, E. Y. (2013). The effect of perceived risk on online shopping in Jordan. *European Journal of Business and Management, 5*(6), 76-87. (ISSN 2222-1905)

Meng, D., Min, Q., & Li, Y. (2008, August). Study on trust in mobile commerce adoption: A conceptual model. In *2008 International Symposium on Electronic Commerce and Security* (pp. 246–249). doi:10.1109/ISECS.2008.54

Mertler, C. A., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods* (5th ed.). Glendale, CA: Pyrczak.

Mitchell, A. F., & Krzanowski, W. J. (1985). The Mahalanobis distance and elliptic distributions. *Biometrika, 72*(2), 464–467. doi:10.1093/biomet/72.2.464

Moghavvemi, S., Salleh, N. A. M., & Abessi, M. (2013). Determinants of IT-related innovation acceptance and use behavior: Theoretical integration of unified theory of acceptance and use of technology and entrepreneurial potential model. *Socialines Technologijos, 3*(2), 243–260. doi:10.13165/ST-13-3-2-01

Morar, D. D. (2013, January). *An overview of the consumer value literature-perceived value, desired value. In the Proceedings of the International Conference*. Marketing-from Information to Decision, 169-186. Babes Bolyai University. Retrieved from https://www.researchgate.net/publication/271585009_An_overview_of_the_consumer_value_literature_-_perceived_value_desired_value

Nuñez, D., & Agudo, I. (2014). BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security, 13*(2), 199–215. doi:10.1007/s10207-014-0230-4

Nunnally, J. C. (1967). *Psychometric theory*. New York, NY, US: McGraw-Hill.

Nunnally, J. (1978). *Psychometric methods*. New York, NY, US: McGraw-Hill.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychological theory*. New York, NY: McGraw-Hill.

Odeyinde, O. B. (2014). *An empirical investigation of the impact of privacy concerns and the unified theory of acceptance and use of technology on location-based services usage intention* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3620149)

Olden, E., Platt, D. C., Royer, C., Berg, K., & Wallingford, J. H. (2015). U.S. Patent No. 8,990,911. Washington, DC: U.S. Patent and Trademark Office. Retrieved from https://patents.google.com/patent/US8990911B2/en

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal Information Systems Evaluation, 14*(1), 110–121. Retrieved from https://www.researchgate.net/publication/258821009

Opala, O. J. (2012). *An analysis of security, cost-effectiveness, and it compliance factors influencing cloud adoption by IT managers* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3527699)

Opala, O. J., & Rahman, S. M. (2013, June). *An exploratory analysis of the influence of information security on the adoption of cloud computing.* In System of Systems Engineering (SoSE), 2013 8th International Conference on (pp. 165-170). IEEE. doi:10.1109/SYSoSE.2013.6575261

Palacios-Marqués, D., Soto-Acosta, P., & Merigó, J. M. (2015). Analyzing the effects of technological, organizational and competition factors on Web knowledge exchange in SMEs. *Telematics and Informatics, 32*(1), 23-32. doi:10.1016/j.tele.2014.08.003

Pandža Bajs, I. (2015). Tourist perceived value, relationship to satisfaction, and behavioral intentions: The example of the Croatian tourist destination Dubrovnik. *Journal of Travel Research, 54*(1), 122–134. doi:10.1177/0047287513513158

Parkin, S., Driss, S., Krol, K., & Sasse, M. A. (2015, December). *Assessing the user experience of password reset policies in a university. In International Conference on Passwords* (pp. 21-38). Springer, Cham. Retrieved from http://discovery.ucl.ac.uk/1473628/1/passwords_2015_final.pdf

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research, 15*(1), 37-59. doi:10.1287/isre.1040.0015

Perera, N. (2017). *Identity and Access Management with GART (GSOC Access Request Tool).* In 68th International Astronautical Congress 2017, IAC 2017. Retrieved from http://elib.dlr.de/116636/1/Identity%20and%20Access%20Management%20with%20GART.pdf

Pérez-Méndez, A., Pereñíguez-García, F., Marín-López, R., & López-Millán, G. (2012). A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network. *International Journal of Information Security, 11*(6), 365–388. doi:10.1007/s10207-012-0174-5

Perry, F., & Pollock, M. (2016). *Digital Identity in Mobile Products for Digital Innovation. International Conference on Information Resources Management Proceedings*. (p. 52). AIS Electronic Library (AISeL). Retrieved from http://aisel.aisnet.org/confirm2016/52

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). *Two-factor authentication: is the world ready?: quantifying 2FA adoption. In Proceedings of the eighth european workshop on system security (p. 4).* ACM. doi:10.1145/2751323.2751327

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. doi:10.1037/0021-9010.88.5.879

Ponte, E. B., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management, 47*, 286-302. doi:10.1016/j.tourman.2014.10.009

Pope, A. D. (2014). *Business intelligence: Applying the unified theory of acceptance and use of technology* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3616064)

Premarathne, U. S., Khalil, I., Tari, Z., & Zomaya, A. (2017). Cloud-based utility service framework for trust negotiations using federated identity management. *IEEE Transactions on Cloud Computing, 5*(2), 290-302. doi.ieeecomputersociety.org/10.1109/TCC.2015.2404816

Protection of Human Subjects, 45 C.F.R. § 46 (2009).

Qualtrics (n.d). Validation. Retrieved from https://www.qualtrics.com/support/survey-platform/survey-module/editing-questions/validation/

Resnik, D. B. (2011). What is ethics in research & why is it important? Retrieved from https://www.niehs.nih.gov/research/resources/bioethics/whatis/

Roberts, P., Priest, H., & Traynor, M. (2006). Reliability and validity in research. *Nursing Standard, 20*(44), 41–45. doi:10.7748/ns2006.07.20.44.41.c6560

Rogers, E. M. (1995). Diffusion of Innovations: Modifications of a model for telecommunications. In Springer (Ed.), *Die Diffusion von Innovationen in der Telekommunikation* (pp. 25-38). Berlin, Germany: Springer.

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). OpenID Connect Core 1.0 incorporating errata set 1. The OpenID Foundation, specification. Retrieved from https://img.sauf.ca/pictures/2017-02-20/a11555bd000b91a19aaad722e8358bf9.pdf

Sánchez-Alzate, J. A., & Sánchez-Torres, J. A. (2017). Analysis of social factors and their relationship with perceived risk for e-commerce purchases. *Dyna, 84*(200), 335-341. doi:10.15446/dyna.v84n200.54161

Sandoval-Almazán, R., & Gil-Garcia, J. (2012). Are government internet portals evolving towards more interaction, participation, and collaboration? Revisiting the rhetoric of e-government among municipalities. *Government Information Quarterly, 29*(1), S72–S81. doi:10.1016/j.giq.2011.09.004

Satchell, C., Shanks, G., Howard, S., & Murphy, J. (2011). Identity crisis: User perspectives on multiplicity and control in federated identity management. *Behaviour & Information Technology, 30*(1), 51–62. doi:10.1080/01449290801987292

Savas, S. (2017). *Perceived risk and consumer adoption of service innovations* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10610496)

Schweighofer, E., & Hötzendorfer, W. (2013). Electronic identities – public or private. *International Review of Law, Computers & Technology, 27*(1/2), 230-239. doi:10.1080/13600869.2013.764142

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems, 19*(1), 93–103. doi:10.1057/ejis.2009.51

Senk, C. (2013). Adoption of security as a service. *Journal of Internet Services and Applications, 4*(11), 1–16. doi:10.1186/1869-0238-4-11

Shang, S. S., & Lin, S. (2010). Barriers to implementing ITIL: A multi-case study on the service-based industry. *Contemporary Management Research, 6*(1), 53–70. doi:10.7903/cmr.1131

Sheng, H., Nah, F., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems, 9*(6), 344–376. Retrieved from http://cbafiles.unl.edu/public/cbainternal/researchlibrary/JAIS_2008_Sheng_Nah_Siau.pdf

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438. doi:10.1016/j.intcom.2010.05.001

Shroff, R. H., Deneen, C. C., & Ng, E. M. (2011). Analysis of the technology acceptance model in examining students' behavioral intention to use an e-portfolio system. *Australasian Journal of Educational Technology, 27*(4), 600–618. doi:10.14742/ajet.940

Slade, E., Williams, M., & Dwivedi, Y. (2014). Devising a research model to examine adoption of mobile payments: An extension of UTAUT2. *The Marketing Review, 14*(3), 310–335. doi:10.1362/146934714X14024779062036

Somorovsky, J., Mayer, A., Schwenk, J., Kampmann, M., & Jensen, M. (2012). On breaking SAML: Be whoever you want to be. In *USENIX Security Symposium* (pp. 397-412). Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91-8-23-12.pdf

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529. doi:10.2307/25148854

Southey, G. (2011). The theories of reasoned action and planned behaviour applied to business decisions: a selective annotated bibliography. *Journal of New Business Ideas & Trends, 9*(1), 43-50. Retrieved from https://pdfs.semanticscholar.org/d7af/d203ec4ce9204bbe26b1c135f478ef9d8aa2.pdf

Steven, J. (2001). *Applied multivariate statistics for the social sciences* (4th ed.) Hillsdale, NJ: Erlbaum.

Stobert, E., & Biddle, R. (2015, December). Expert password management. In International Conference on Passwords (pp. 3-20). *Springer, Cham*. Retrieved from https://www.cl.cam.ac.uk/events/passwords2015/preproceedings.pdf

Straub, E. T. (2009). Understanding technology adoption: Theory and future directions for informal learning. *Review of Educational Research, 79*(2), 625–649. doi:10.3102/0034654308325896

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston, MA: Allyn & Bacon.

Tadesse, Y. (2012). *An investigation of influencing factors for adopting federated identity authentication in service-oriented architecture (SOA)*. (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3498092)

Tagler, M. J., Stanko, K. A., & Forbey, J. D. (2017). Predicting sleep hygiene: A reasoned action approach. *Journal of Applied Social Psychology, 47*(1), 3–12. doi:10.1111/jasp.12411

Tan, P. J. B. (2013). Applying the UTAUT to understand factors affecting the use of English e-learning websites in Taiwan. *Sage Open, 3*(4), 1-12. doi:10.1177/2158244013503837

Tate, M., Evermann, J., & Gable, G. (2015). An integrated framework for theories of individual attitudes toward technology. *Information & Management, 52*(6), 710–727. doi:10.1016/j.im.2015.06.005

Temoshok, D., & Abruzzi, C. (2016). *Developing trust frameworks to 5 support identity federations.* Washington, DC: National Institutes of Standards and Technology. Retrieved from https://csrc.nist.gov/csrc/media/publications/nistir/8149/draft/documents/nistir_8149_draft.pdf

Thibeau, D. (2016). Innovations in federation: global interoperability. Retrieved from http://events.afcea.org/GlobalID16/CUSTOM/pdf/innov-in-federation.pdf

Tinsley, H. E., & Tinsley, D. J. (1987). Uses of factor analysis in counseling psychology research. *Journal of Counseling Psychology, 34*(4), 414-424. doi:10.1037/0022-0167.34.4.414

Tmušić, M., Veinović, M. (2017). Managing Risks by Federating Identities in Digital Economy. Paper presented at Sinteza 2017 - *International Scientific Conference on Information Technology and Data Related Research*. doi:10.15308/Sinteza-2017-30-34

Tornatzky, L., & Fleischer, M. (1990). The process of technology innovation, Lexington, MA. Lexington Books. Trott, P. (2001). The Role of Market Research in the Development of Discontinuous New Products. *European Journal of Innovation Management, 4*(3), 117-125. doi:10.1108/14601060110390585

Tran, Q., Zhang, C., Sun, H., & Huang, D. (2014). Initial adoption versus institutionalization of e-procurement in construction firms: An empirical investigation in Vietnam. *Journal of Global Information Technology Management, 17*(2), 91–116. doi:10.1080/1097198X.2014.928565

Tschofenig, H., Falk, R., Peterson, J., Hodges, J., Sicker, D., & Polk, J. (2006). Using SAML to protect the session initiation protocol (SIP). *IEEE Network, 20*(5), 14–17. doi:10.1109/MNET.2006.1705878

Tuan Mat, T. (2010). Management accounting and organizational change: impact of alignment of management accounting system, structure and strategy on performance. Retrieved from http://ro.ecu.edu.au/theses/149

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology, 52*(5), 463–479. doi:10.1016/j.infsof.2009.11.005

U.S. Department of Health and Human Services. (1979). The Belmont report (45 CFR 46).

VanVoorhis, C. W., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. *Tutorials in Quantitative Methods for Psychology, 3*(2), 43-50. doi:10.20982/tqmp.03.2.p043

Vedenhaupt, L. L. (2016). *Analyzing the relationship between social media usage and ticket sales at small nonprofit performing arts organizations* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10061501)

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273–315. doi:10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 4692,* 186–204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh, V., Davis, F. D., & Morris, M. G. (2007). Dead or alive? The development, trajectory and future of technology adoption research. *Journal of the Association for Information Systems, 8*(4), 267–286. Retrieved from http://www.vvenkatesh.com/wp-content/uploads/2015/11/VenkateshetalJAIS2007.pdf

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly, 27*(3), 425–478. doi:10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178. Retrieved from https://ssrn.com/abstract=2002388

Vogt, W. P. (2007). Quantitative research methods for professionals. Boston, MA: Pearson Education

Vijay, V., Durbhakula, K., & Kim, D. J. (2011). E-business for nations: A study of national level e-business adoption factors using country characteristics-business-technology-government framework. *Journal of Theoretical and Applied Electronic Commerce Research, 6*(3), 1–12. doi:10.4067/S0718-18762011000300002

Wang, R., Chen, S., & Wang, X. (2012, May). Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. In *Security and Privacy (SP),* 2012 IEEE Symposium on (pp. 365-379). IEEE. doi:10.1109/SP.2012.30

Wang, Y. S., Li, H. T., Li, C. R., & Zhang, D. Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment framework. *Tourism Management, 53,* 163–172. doi:10.1016/j.tourman.2015.09.021

Wen, K. W., & Chen, Y. (2010). E-business value creation in Small and Medium Enterprises: a US study using the TOE framework. *International Journal of Electronic Business, 8*(1), 80-100. doi:10.1504/IJEB.2010.030717

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample size requirements for structural equation models: An evaluation of power, bias, and solution propriety. *Educational and Psychological Measurement, 76*(6), 913–934. doi:10.1177/0013164413495237

Wolf, M., Thomas, I., Menzel, M., & Meinel, C. (2009, January). A message meta model for federated authentication in service-oriented architectures. In *The 2009 IEEE International Conference on Service-Oriented Computing and Applications* (pp. 1–8). doi:10.1109/SOCA.2009.5410466

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers’ adoption of location-based services. *Electronic Markets*, *19*(2-3), 137–149. doi:10.1007/s12525-009-0012-4

Xu, X. (2013). *Development of a new mobile application to predict theme park waiting time.* (Doctoral dissertation). Available from Graduate Dissertation, Iowa State University Digital Repository. Retrieved from http://lib.dr.iastate.edu/etd/13586

Zaiţ, A., & BERTEA, P. S. P. E. (2011). Methods for testing discriminant validity. *Management & Marketing Journal*, *9*(2), 217–224. Retrieved from https://www.researchgate.net/profile/Adriana_Zait/publication/227367690_Methods_for_Testing_Discriminant_Validity/links/00b49528ef773b42af000000.pdf

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *Journal of Marketing*, *52*(3), 2–22. doi:10.2307/1251446

Zhou, T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research*, *13*(2), 135–144. Retrieved from http://www.jecr.org/sites/default/files/13_2_p03.pdf

Zhu, K., Kraemer, K. L., & Dedrick, J. (2004). Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of management information systems, 21*(1), 17-54. doi:10.1080/07421222.2004.11045797

# STATEMENT OF ORIGINAL WORK

## Academic Honesty Policy

Capella University's Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.

Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person's ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others' work through proper citation and reference. Use of another person's ideas, including another learner's, without proper reference or citation constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else's ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University's Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

## Statement of Original Work and Signature

I have read, understood, and abided by Capella University's Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Learner name
and date Bunmi Samuel 1/8/2018

# APPENDIX A. RESEARCH INSTRUMENT

1. Please select the answer that best describes your gender:
   1:Male
   2:Female
2. Please select the answer that best describes your age:
   1:< 21
   2:21 – 30
   3:31 – 40
   4:41 – 50
   5:51 – 60
   6:61 - 70
3. Please select the answer the best describes your ethnicity:
   1:White/Caucasian
   2:American Indian
   3:Asian
   4:Hispanic/Latino
   5:African American
   6:Pacific Islander
   7:Other
4. Have you earned any academic degrees outside the United States?
   1:Yes
   2:No
5. Please select the answer that best describes your education:
   1:High School/GED or Less
   2:Associate
   3:Bachelors
   4:Masters
   5:PhD
   6:Other Post Graduate Degree
6. What is the primary major of the latest degree program you completed?
   1:Science
   2:Engineering
   3:Other Technical
   4:Business
   5:Arts
   6:Other
7. What is your occupational title?
   1:Chief Information Officer (CIO)
   2:Chief Information Security Officer (CISO)
   3:Director of IT
   4:IT Manager
   5:IT Team Lead/Supervisor
   6:Enterprise Architect

7:Vice President of IT
8:Project Manager
9:Other, please specify

8. How many years of experience do you have in making IT decision for your organization?
    1. < 2 years
    2. 2 – 5 years
    3. 5 – 10 years
    4. 10 – 15 years
    5. More than 15 years
    6. Other, please specify
9. What is the approximate number of users supported by your organization?
    1. < 500
    2. 501 – 1,000
    3. 5001 – 10,000
    4. 10,001 – 20,000
    5. More than 20,000
10. Please select the answer that best describes your annual household income:

1:Less than $60,000
2:$60,001 - $80,000
3:$80,001 - $100,000
4:$100,001 - $120,000
5:$121,001 - $140,000
6:$141,001 - $160,000
7:$161,001 - $180,000
8:$181,001 - $200,000
9:Greater than $200,000

Please indicate the degree to which you agree or disagree with statement based on 5-point Likert scale e.g. 1 = Strongly Disagree (SD), 3 = Neutral (N) and 5 = Strongly Agree (SA)

1: Strongly Disagree
2: Somewhat Disagree
3: Neither Agree nor Disagree
4: Somewhat Agree
5: Strongly Agree

**Performance Expectancy (PEE) (adapted from Zhou, 2012)**

Performance Expectancy (PEE): is the degree to which individual beliefs that using and accepting the system will help him or her to attain gains in job performance. In light of the statement above, please, express your level of agreement with the following statement:

- PEE1: Using FIM improves my living and working efficiency.
- PEE2: Using FIM increases my living and working productivity.
- PEE3: I find that FIM is useful.

**Effort Expectancy (EFE) (adapted from Zhou, 2012)**

Effort Expectancy is the degree of ease associated with the use and accepts of the system. Considering the statement above, please, express your level of agreement with the following statement:

- EFE1: Learning to use FIM is easy for me.
- EFE2: Skillfully using FIM is easy for me.
- EFE3: I find that FIM is easy to use.

**Social influence (SOI) (adapted from Zhou, 2012)**

Social Influence (SOI): the degree to which an individual perceives that others believe he or she should use a particular system. In light of the statement above, please, express your level of agreement with the following statement:

- SOI1: People who influence my behavior think that I should use FIM.
- SOI2: People who are important to me think that I should use FIM.

**Facilitating conditions (FAC) (adapted from Zhou, 2012)**

Facilitating Conditions (FAC): the degree to which an individual belief that an organizational and technical infrastructure exists to support the use of a particular system. Considering the statement above, please, express your level of agreement with the following statement:

- FAC1: I have the resources necessary to use FIM.
- FAC2: I have the knowledge necessary to use FIM.
- FAC3: A specific person (or group) is available for assistance with FIM system difficulties.

**Trust (TRU) (adapted from Zhou, 2012)**

Trust (TRU): Is the strong confidence in the capability of an individual or organization to act reliably and dependably within a specific situation. In light of the statement above, please, express your level of agreement with the following statement:

- TRU1: This service provider is trustworthy.
- TRU2: This service provider keeps its promise.
- TRU3: This service provider keeps customer interests in mind.

**Security (SEC) (Adapted from Opala, 2012)**

Security Concern (SEC): is a concrete technical characteristic, given when a certain technological solution responds to all of five security objectives: confidentiality, authentication, integrity, authorization, and non-repudiation. Considering the statement above, please, express your level of agreement with the following statement:

- SEC 1:  I feel that FIM is secure.
- SEC 2: I am concerned about the security of the technology used in the FIM.
- SEC 3: I feel that FIM is more secure than the traditional authentication methods
- SEC 4: I am willing to use FIM to access sensitive information for my organization

**Privacy concern (PRC) (adapted from Zhou, 2012)**

Privacy (PRI): the ability of the individual to control the terms under which personal information is acquired and used. Considering the statement above, please, express your level of agreement with the following statement:

- PRC1: I am concerned that the information I disclosed to the service provider could be misused.
- PRC2: I am concerned that a person can find private information about me on the Internet.
- PRC3: I am concerned about providing personal information to the service provider, because of what others might do with it.
- PRC4: I am concerned about providing personal information to the service provider because it could be used in a way I did not foresee.

**Perceived risk (RISK) (adapted from Zhou, 2012)**
Perceived Risk (PER): is a disclosure of personal information when using technology which causes users to be pessimistic about future impacts of such disclosure. In light of the statement above, please, express your level of agreement with the following statement:

- PER1: Providing this service provider with my personal information would involve many unexpected problems.
- PER2: It would be risky to disclose my personal information to this service provider.
- PER3: There would be a high potential for loss in disclosing my personal information to this service provider.

**Behavior Intention to Adopt FIM (BI) (adapted from Zhou, 2012)**
Behavioral Intention (BIA): as a person's perceived likelihood or subjective probability that he or she will engage in a given behavior. Considering the statement above, please, express your level of agreement with the following statement:

- BIA1: I intend to use FIM in the next <n> months.
- BIA2: I predict I would use FIM in the next <n> months.
  BIA3: I plan to use FIM in the next <n> months