ABSTRACT

The technological revolution that has taken place in the latter part of the twentieth and the beginning of the twenty first century has opened new pathways for technological advancements. New fields within the broad spectrum of information technology are being introduced and researched upon. This has not only changed the daily lives of human beings but also contributed to the transformation in the financial system.

Things that would probably be considered magic in the middle of the twentieth century are not only being visualized but even implemented. Fields such as machine learning and artificial intelligence have advanced from basic mathematical models to the solution of complex cognitive problems. The singularity point at which machine intelligence surpasses human intelligence is being discussed as a probability.

The field of information technology can be considered as a broad spectrum of fields that have, in many cases, very distinct objectives. One such emerging field is IoT or the internet of things. It is concerned with the communication of electrical components and sensors in a network to serve the purpose of data-sharing and dependent decision-making.

This study primarily concerns itself with the study of human behaviors that contribute to the acceptance of technology in their daily life. The research is conducted primarily in the technological context of “internet of things”. Concerns regarding the security of data in the sphere of IoT are also discussed in detail in this study.

Multiple theories have been developed over the years regarding the factors that influence user’s decisions. One of the most famous ones is UTAUT (Unified theory of acceptance and use of technology) developed and published in 2016, that aims to explain the issues that users address when accepting or rejecting a technology. This study will review the theory in detail and will address the aspects applicable to our study.

DEDICATION

This research is dedicated to my parents, who have been the source of motivation and inspiration for this study. A work of this magnitude would not have been possible without their generous support and consistent cooperation.

I would also like to dedicate this work to my siblings, peers, mentors, friends, and classmates who shared their advice and encouraged me to conduct this study. TBD

ACKNOWLEDGEMENTS

For the completion of this study, I would like to thank my instructors, namely ,who have guided and supported me through the narrow and dark roads of research. I would also like to thank my colleagues, , who motivated and assisted me on this arduous journey. Apart from them, I would like to thank my friends, for their constant encouragement. TBD

TABLES OF CONTENTS

CHAPTER 1: INTRODUCTION

Problem Statement and Background of the Problem 1

Significance of the Study 3

Theoretical Framework – Theories of User Acceptance of Technology 4

Researcher’s Positionality (Role of the Researcher) 5

Purpose of the Study 5

Research Question and Hypotheses 5

Rationale for Methodology and Design 6

Operational Definitions for the Study 7

Assumptions and Limitations 8

Organization of the Study 9

CHAPTER 2: LITERATURE REVIEW

Chapter Overview 11

Extensiveness of the Literature 11

Theoretical Framework – Theories of Use Acceptance of Technology 11

TRA 12

TPB 12

IDT 12

TAM 12

Review of the Seminal Literature 13

Background of the Problem 13

Examples of IoT/Smart Technology 13

Three variables Affecting the Adoption of IoT 14

Review of the Practitioner Literature 15

The Internet of Things (IoT) and Smart Technology 15

Applications of IoT/Smart Technology 15

Smart Things 16

Smartphones 16

Smart clothing 16

Smart appliances 17

Smart homes 17

Smart buildings 18

Smart grids 18

Smart cities 18

Smart transportation systems 19

Smart automobiles 19

Smart medical and health care 20

Smart cost control 20

Smart quality of service 21

Microcontrollers 21

Computing and networking 22

Cellular networks 23

WiFi 23

Zigbee 23

Bluetooth 23

6LoWPAN 24

Architecture of the IoT 25

Edge layer 25

Access gateway layer 25

Middleware layer 25

Application layer 26

Security and identity links 26

General Security Concerns of the IoT 27

Assets 27

Vulnerabilities 28

Current Threats 28

Future threats 28

Consequences of Threats 28

Compromise 29

Privilege escalation 29

Impersonation 30

Persistence 30

Data discovery 30

Data Tampering 30

Man in the middle 31

Denial of service 31

Specific Security Issues of the IoT 31

Embedded security issues 31

Wireless security issues 32

Monitoring Challenges 32

Big-data Problems 32

Secure framework designs 33

Autonomous computing 34

Privacy 34

Safety 35

Practical Issues of the IoT 36

Standardization 36

Fault tolerances 37

Interoperability 37

Trust 38

Governance challenges of the IoT 38

Security program management 38

Security policies 39

Security Education, Training, and Awareness (SETA) 40

Monitoring of policy 40

Information security governance of the IoT 41

Organization effects of the IoT on policy 41

Cultural effects of the IoT on policy 42

CHAPTER 3: METHODOLOGY

Chapter Overview 43

Statement of the Problem, Research Question(s), and Hypotheses 43

Research Methodology 44

Research Design 44

Sample Selection 44

Instrumentation 45

Validity and Reliability 47

Data Collection Procedures 48

Data Analysis Procedures 48

Ethical Considerations and Procedures 49

CHAPTER 4: DATA RESULTS AND ANALYSIS

Data Results TBD

Descriptive Statistical Analysis TBD

Descriptive Analysis TBD

Hypothesis Testing TBD

Themes TBD

Data Findings TBD

Findings of the Study TBD

CHAPTER 5: IMPLICATIONS AND CONCLUSIONS

Fulfillment of Research Purpose TBD

Implications for Business Practice TBD

Implications for Research TBD

Conclusions TBD

LIST OF TABLES

Table 1. Title

Table 2. Title

APPENDICES

APPENDIX A – “Smart Technology” and IoT Use Survey 63

LIST OF ACRONYMS

CFA Confirmatory Factor Analysis

EE Effort Expectancy

FC Facilitating Conditions

GSM Global System for Mobile communication

IDT Innovation Diffusion Theory

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

IT Information Technololgy

M2M machine-to-machine

MTU Maximum Transmission Unit

PCU Personal Computer Utilization

PHI personal health information

PII personally identifiable information

PU Perceived usefulness

QoS Quality of Service

REST Representational State Transfer

RFID Radio Frequency Identification

SCT Social Cognitive Theory

SEM Structural Equation Modeling

SETA Security Education, Training, and Awareness

SI Social Influence

SIEM Security Information Event Management

SPSS Statistical Package for the Social Sciences

TAM Technology Acceptance Model

TPB Theory of Planned Behavior

TRA Theory of Reasoned Action

UTAUT Unified Theory of Acceptance and Use of Technology

## 

## CHAPTER 1: INTRODUCTION

The rapidly advancing field of Internet of technology (IoT) has extraordinary potential but carries with it many issues that may deleteriously affect user privacy, safety, and especially security (Atzori et al., 2010). Researchers have discovered that users frequently minimize this concern for security in favor of convenience and ease of use of the technology and that they expect ownership and security of their smart devices and data. (Bandyopadhyay and Sen, 2011). The Internet of Things (IoT), also known as internet-connected devices and more commonly known as “smart technology”, can be described as the collection of interconnected devices using internet technologies, such as Nest thermostat, Google assistant, Amazon Alexa, Nest Secure Alarm, Apple HomePod. These connected devices have embedded wireless modules that hold capabilities of processing, sharing and communicating information to other devices in the network and users (Bojanova, Hurlburt, & Voas, 2014).

The Internet of Things is a key technology for digital businesses. The companies that make the fusion of the worlds, between the physical and the digital, must master taking advantage of the strategies generated around the IoT. Research indicates that users expect ownership and security of their smart devices and data lost (Bandyopadhyay and Sen, 2011),

Examples of the Internet of Things includeAlexa, Nike Fuelband, Google Glass, Fitbit, Apple HomePod, Nest Secure Alarm and Google Assistant. An important feature of the IoT is the potential for smart devices, communicating with different devices, to give significant data and utility to their human users (Dlodlo, Foko, Mvelase, and Mathaba, 2012). Likewise, as the old technologies before it, the IoT may grow more than anybody can predict as of now. Despite the fact that the IoT technology indicates huge potential, there are numerous security issues with the IoT, which may affect its acceptance and adoption by the users (Atzori, Iera, and Morabito, 2010). Eventually, the IoT will empower the independent connectivity of those devices, without human interaction (Dlodlo et al., 2012).

### Background of the Problem

Internet of Things includes two ideas – connectedness and individual items (Atzori et al., 2010). Atzori et al. (2010) said that adoption of the technology would be slowed down if the security issues were not resolved. The combination of remote devices with weak control and handling make the IoT defenseless against security issues (Atzori et al., 2010). Security issues of the IoT include privacy, confidentiality, and accessibility (Ning, Liu, and Yang, 2013). At the point when IoT data travel through public networks and systems, it is vulnerable to denial of service and man in the middle attacks (Hurlburt, Voas, and Miller, 2012). Another example is that the utilization of RFID (Radio Frequency Identification) labels in the healthcare industry is normal; however, there are not huge security and privacy issues that need to be resolved (Han, Chu, and Luo, 2011). If personnel data of patients will be leaked to unauthorized personnel than it might lead to dangerous situation for the relative hospital.

Some researchers have discovered that users exchange security and privacy for the sake of convenience and comfort in use of devices (Bojanova et al., 2014). With the collection and leakage of confidential data, for example, personal health information, personally identifiable information and other private data, the IoT can possibly hurt users more than encourage them. Therefore, the suitability of this analysis as the Internet of Things is growing cannot be neglected.

By better understanding the elements driving adoption of the IoT, including security, cost, and quality awareness, changes might be made sooner, to increase the adoption rate of the technology and prevent delays in adoption. Since the technology is as still growing and developing, this is the ideal opportunity to affect changes.

From a business and security perspective, the topic is relevant to IoT vendors, service suppliers, and business managers as they struggle to offer IoT items to customers. Atzori et al. (2010) said that few technology and social issues, including "trust, protection, and security" should be sorted out before IoT will be "broadly acknowledged" (p. 2788).

### Problem Statement and Significance of the Study

The rapidly advancing field of Internet of technology (IoT) has extraordinary potential but carries with it many issues that may deleteriously affect user standardization, scalability, privacy, safety, and especially security (Atzori et al., 2010). Researchers have discovered that users frequently minimize this concern of security in favor of convenience and ease of use of the technology.

The results of this study may help in defining other factors that can influence acceptance of IoT technology. The results may also reveal other elements of technology adoption that surpass the impact of security, cost and quality awareness.

The relationship between customer security awareness and adoption of IoT is significant, as an understanding of this relationship will turn out to be increasingly important as more security issues are found. From a research perspective, this study is significant for two reasons. To begin with, the topic can possibly broaden a behavioral expectation model to clarify the phenomena of the five factors with regards to adopting the IoT. Furthermore, the study helps to fill the gap left in study of adoption of IoT technology by the other researches. Along these lines, this research meets those gaps. Given the possibility to adjust the available theories to better understand issues regarding IoT adoption, the study will be able to address all the gaps left by previous studies (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014). By applying the construct of Security Awareness, data collection, purchase cost, quality of service and easy-of-use to the unified theory of acceptance and utilization of technology, the model might be utilized by others to better understand the technology adoption.

By evaluating the connection between awareness of security issues and goal to adopt the IoT, business managers and IoT vendors may better upgrade devices and accordingly improve adoption of the technology. This means that companies must discover how to create the next generation of products and services for customers before competitors do.

**Theoretical Framework – Theories of Acceptance of Technology**

This study will be framed in the Unified Theory of Acceptance and Utilization of Technology (UTAUT) as posited by Venkatesh, Morris, Davis, and Davis (2003) and revised in 2012 by Venkatesh, V., L. Thong, J. Y., & Xu, X.. (2012). The UTAUT aims to explain user intentions to use an information system and subsequent usage behavior. The theory posits that four key constructs -- performance expectancy, effort expectancy, social influence, facilitating conditions, (trust was added in a later model) – can explain one’s intentions to use an information system and one’s subsequent usage behavior. Constructs performance expectancy, effort expectancy, and social influence are direct determinants of user intention and user behavior and the construct social influence is a direct determinant of user behavior. The theory further posits that the effect of the four constructs on intention and behavior is moderated by gender, age, experience, and voluntariness of use. According to Thomas, T., Singh, L., and Gaffar K. (2013), the UTAUT model draws on the Theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM), the Motivational Model, the Theory of Planned Behavior (TPB), the combined TAM and TPB, the model of Personal Computer Utilization, the Innovation Diffusion Theory and the Social Cognitive Theory and uses behavioral intention as a predictor as a predictor of technology use behavior. Thomas, et al. (2013) further state that subsequent validation of UTAUT in a longitudinal study found it to account for 70% of the variance in Behavioral Intention to Use (BI) and about 50% in actual use. A detailed discussion of UTAUT and its link to this study is presented in Chapter 2 – Literature Review, heading Theoretical Framework – UTAUT.

**Researcher’s Positionality**

As this will be a quantitative study based on statistical analysis of numerical responses on a questionnaire, the researcher will assume a purely objective role in running the statistics and presenting the tables of results. However, to interpret resulting statistics as they apply to answering the research question will involve some degree of subjectivity based on the researcher’s knowledge of the subject. Being aware of the pitfalls of subjectivity, the researcher will endeavor to insure any interpretation is within context of the research question.

**Purpose of the Study**

The primary purpose of this quantitative, correlational, non-experimental study will be to determine to if a user’s perception of the perceived usefulness, effort expectancy, social influence, facilitating conditions, and trust of the Smartwatch are significant predictors of a consumer’s adoption of the smartwatch in daily activities. A smartwatch is a wearable computer in the form of a wristwatch that tracks fitness, monitors health, gives quick access to notifications, and also tells time. Smartwatches provide a local touchscreen interface for daily use while an associated smartphone app provides for management and telemetry (such as long-term biomonitoring). Apple, Samsung, Sony, and others offer smartwatches on the consumer market. Pebble announced its first smartwatch in 2013 and raised a record amount of funding on Kickstarter going on to sell more than 1 million units.

Gao and Bai (2014) suggest there is an absence of research on the variables affecting adoption of the IoT. Further, the investigation will explain the elements a user considers while accepting the IoT. With the collection and leakage of confidential data, for example, personal health information, personally identifiable information and other private data, the IoT can possibly hurt users more than encourage them. Therefore, the suitability of this analysis as the Internet of Things is growing cannot be neglected (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Research Question and Hypotheses**

Do perceived usefulness, effort expectancy, social influence, facilitating conditions, and trust of the Smartwatch predict a consumer’s adoption of the smartwatch? The dependent variable is a consumer’s use of a Smartwatch (as measured by level of usage questions from the UTAUT). (See Appendix A – “Smart Technology” and IoT Use Survey). The independent variables are consumers’ perceived usefulness, effort expectancy, social influence, facilitating conditions, and trust of the Smartphone (as measured by the UTAUT (See Appendix A – “Smart Technology” and IoT Use Survey).

To answer this question, three statistical hypotheses will be tested.

* H1: Perception of usefulness of the Smartwatch is a statistically significant predictor of a consumer’s adoption of the Smartwatch.
* H2: Effort expectancy in using of a Smartwatch is a statistically significant predictor of a consumer’s adoption of the Smartwatch.
* H3: Social influence is a statistically significant predictor of a consumer’s adoption of a Smartwatch.
* H4: Facilitating conditions is a statistically significant predictor of a consumer’s adoption of a Smartwatch.
* H5: Trusts is a statistically significant predictor of a consumer’s adoption of a Smartwatch.

The statistical hypotheses will be tested using a multiple, linear regression hosted on SPSS™. A detailed description of the hypotheses and data analysis is presented in Chapter 3 – Methodology.

**Rationale for Methodology and Design**

This will be a quantitative, correlational, non-experimental study. The study is quantitative in that it will ask respondents to indicate their perceptions of specific items numerically and not verbally. The study is correlational in that it will measure the statistical correlation between numerical responses of items. The study is non-experimental in that is does not attempt to determine if a specific variable causes a specific effect. The choice of a quantitative, non-experimental correlational design is consistent with other designs used to advance understanding of the quantitative nature of relationships between a participant’s perception of specific items, such as use of IoT and perception of security in this study. Chu (2015) stated that quantitative studies are used to logically prove and scientifically verify theories. Babbie (1983) stated that quantitative research is “the numerical representation and manipulation of observations for the purpose of describing and explaining the phenomena that those observations reflect” (p. 537). Using a quantitative design allows researchers to obtain numerical data from which usable statistics can be developed through statistical analysis (Groeneveld, Tummers, Bronkhorst, Ashikali, & Van Thiel, 2015). The primary statistical procedure will be multiple linear regression and is most appropriate for cases, such as this research, where the DVs have more than one cause and those causes, as represented by IVs, are inter-correlated (McClendon, 1994).

### Operational Definitions for the Study

Following are definitions of key terms used in this study:

*Internet of Things (IoT).* “The Internet of things (IoT) is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data”. (Wikipedia)

*U.S. Consumers.* Only U.S customers will be considered for the purpose of this study and participants of age 18 or more will be involved. Furthermore, IoT smart devices users or potential users will be selected for the study.

*Technology Adoption.* From a technology adoption point of view, achievement is characterized as the degree a framework is preferred and exceptionally utilized by users (V. Venkatesh et al., 2003). Various models have been created to quantify user adoption of technology. The Technology Acceptance Model (TAM), created by Davis (1989) is likely the most generally utilized model (Abu-Al Aish and Love, 2013). Expanding on the TAM and seven different models, the unified theory of acceptance and utilization of technology plans to better explain technology adoption.

### *Performance expectancy (PE):* “the degree to which an individual believes that using the system will help him or her to attain gains in job performance” (Venkatesh et al. 2003, pp 447-453).

### *Effort expectancy (EE):* “the degree of ease associated with use of the system” (Venkatesh et al. 2003, pp 447-453);

### Social influence (SI): “the degree to which an individual perceives that important others believe he or she should use the new system”; and (Venkatesh et al. 2003, pp 447-453)

### *Facilitating conditions (FC):* “the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system”

### *Gender:* The sex of the user.

### *Age:* How old the user is.

### *Experience:* the amount of experience a use has in using technology.

### *Voluntariness of use:* the extent to which a choice being made is of a person's free will as opposed to being made as the result of coercion or duress. (Venkatesh et al. 2003, pp 447-453).

### Assumptions and Limitations

It is assumed that participants will sincerely answer the survey questions. It is assumed that participants will answer questions to the best of their capacity and give answers that are true reflection of their conduct. It is also assumed that the model can be modified to measure the added variable of security awareness.

Likert Scale data are assumed to be valid measures of ordinal data on a interval (scale) level as long as they declared equal distance among levels and the instrument is used in a summative way (Allen and Seaman, 2007). At the point when these two assumptions are not made, Likert data are viewed as ordinal data and in this way nonparametric statistical techniques should be utilized. Correlation and regression are genuinely strong (Allen and Seaman, 2007).

**Summary and Organization of the Study**

This study is organized into five chapters as follows:

Chapter 1 – Introduction. This chapter introduces the problem of IoT, states the research question, identifies the significance of the study, and explains the research design used to answer the question.

Chapter 2 – Literature Review. This chapter provides an overview of the background to the problem, supports the statements and inferences of the negative results of the problem, describes in detail the research framework for the study, and presents results of studies about the problem and their connection to the research question.

Chapter 3 – Methodology. This chapter describes in detail the research method used, defines the variables and explains how they were measured, describes the data collection instruments, explains the statistical procedure used to analyze the data, and defines the decision rule for determining the answer to the research question, and discusses protection of human and animal subjects and the validation of results.

Chapter 4 – Findings. This chapter presents the findings of this research in table and graphical format and narrative, including interpretation of the data.

Chapter 5 – Summary and Conclusions. This chapter summarizes the findings from the research, states conclusions drawn from the research, provides a direct answer to the research question, and discusses in detail the links to prior research and implications for the field of study.”

## CHAPTER 2: LITERATURE REVIEW

**Chapter Overview**

This chapter presents a detailed discussion of the problem of adoption of IoT technology and a detailed description of what IoT is, how it works, its pervasiveness in society, and its issues.

### Strategy for Identifying Applicable Research

The strategy to review the literature was based on searching for literature about the primary variables of interest for this study to include IoT security, ease of use of IoT, purchase cost of IoT service, consumers’ adoption and acceptance of IoT. Primary sources of literature relevant to this study included Cordia University Library, Google Scholar, Ebsco Host, specific online journals, and the internet. Literature was also sought to explain the theoretical framework of this study and relate it to the research question to include the Theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM), the Motivational Model, the Theory of Planned Behavior (TPB), the model of Personal Computer Utilization, the Innovation Diffusion Theory and the Social Cognitive Theory. Key search terms used included: IOT, smart technology, internet of things, UTAUT, and adoption of technology. The literature presented spans the last 30 years with most of the studies being in the last 10 years. Literature includes published data from government and official sources, presentations of statistical and qualitative research studies, and published articles summarizing research findings and reviews and presentations of some of the seminal literature on the topic.

### Extensiveness of the Literature Review

The literature reviewed fell into three basic categories as suggested by the nature of this study: literature about the problem (i.e., technology security), literature about the research framework (i.e., the acceptance of technology), and literature about the state of the technology. As the technology discussed in this study changes quickly, currency of the literature about the technology is important. Thus, as posted in the References section of this document, 50 sources referred and cited were published after 2011 (i.e., less than seven years old) with other corroborating sources within the last 20 years to demonstrate the evolution of the problem, framework, and technology. Some of the sources regarding statistics and the methodology (see Chapter 3 – Methodology) are older but are still considered relevant and seminal in that questionnaire structure, statistical procedures, and calculations have essentially not changed. Many of the sources reviewed were citing the same sources and after reviewing over 100 sources, the current list was considered to be representative of the vast majority of the literature.

**Review of the Seminal Literature**

Seminal works of literature are those works recognized as important landmarks in scholarship and “promote a new theory that becomes an acceptable and valid perspective that all future scholars must read and incorporate into their understanding of the field in order to conduct informed research projects . . . required to establish the conceptual framework of a dissertation.” (Grand Canyon University, 2019, p. 4). Following is a review of the seminal literature organized to present a detailed background of the problem.

**Theoretical Framework – Theories of User Acceptance of Technology**

This study dealing with the adoption of technology to IoT is framed in the Unified Theory of Acceptance and Utilization of Technology (UTAUT) as posited by Venkatesh, Morris, Davis, and Davis (2003) and revised in 2012 Venkatesh, V., L. Thong, J. Y., & Xu, X.. 2012). The UTAUT aims to explain user intentions to use an information system and subsequent usage behavior. Perceived ease of use is portrayed as influencing both perceived usefulness and behavioral intent (Gangwar, Date, and Raoot, 2014).

**UTAUT** **Model of Acceptance of Technology**

The UTAUT theory posits that four key constructs -- performance expectancy, effort expectancy, social influence, facilitating conditions – can explain one’s intentions to use an information system and one’s subsequent usage behavior. Constructs performance expectancy, effort expectancy, and social influence are direct determinants of user intention and user behavior and the construct social influence is a direct determinant of user behavior. The theory further posits that the effect of the four constructs on intention and behavior is moderated by gender, age, experience, and voluntariness of use.

According to Thomas, T., Singh, L., and Gaffar K. (2013), the UTAUT model draws on the Theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM), the Motivational Model, the Theory of Planned Behavior (TPB), the combined TAM and TPB, the model of Personal Computer Utilization, the Innovation Diffusion Theory and the Social Cognitive Theory and uses behavioral intention as a predictor as a predictor of technology use behavior. Thomas, et al. (2013) further state that subsequent validation of UTAUT in a longitudinal study found it to account for 70% of the variance in Behavioral Intention to Use (BI) and about 50% in actual use.

Figure 1 – UTAUT Model depicts the connections of the various factors to the two primary things “Behavioral Change” and “Use Behavior”. The UTAT model predicts behavioral change and use behavior from four core constructs – Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions – and is moderated by four other variables – gender, age, experience with technology, and “voluntariness” of use.

**Voluntariness**

**of Use**

**Gender**

**Age**

**Experience**

**Performance**

**Expectancy**

**Effort**

**Expectancy**

**Social**

**Influence**

**Facilitating**

**Conditions**

**Behavioral**

**Change**

**Use**

**Behavior**

*Figure 1. UTAUT Model.* (Venkatesh et al. 2003)

*Performance expectancy (PE):* “the degree to which an individual believes that using the system will help him or her to attain gains in job performance”;

*Effort expectancy (EE):* “the degree of ease associated with use of the system”;

*Social influence (SI):* “the degree to which an individual perceives that important others believe he or she should use the new system”; and

*Facilitating conditions (FC):* “the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system”

*Gender:* The sex of the user.

*Age:* How old the user is.

*Experience:* the amount of experience a use has in using technology.

*Voluntariness of use:* the extent to which a choice being made is of a person's free will as opposed to being made as the result of coercion or duress. (Venkatesh et al. 2003, pp 447-453).

The arrows in the model indicate that:

* only Performance Expectancy, Effort Expectancy, and Social Influence predict Behavioural Change;
* Facilitating Conditions only predicts Use Behaviour;
* only gender and age moderate Performance Expectancy;
* only gender, age and experience moderate Effort Expectancy;
* only gender, age, and experience moderate Social Influence;
* voluntariness of use only moderates Behavior Change. and
* only age and experience moderate actual Use Behavior.

Venkatesh et al. (2003) indicate that the UTAUT model explains approximately 70% of the variance in behavioral intention, although other studies have found “lower explanatory powers; 64.5% (Wang & Shih 2009), 63.1% (Al-Gahtani, Hubona, & Wang 2007), 35.3% without interactions and 39.1% with interactions (Teo 2011). “ (as cited in Thomas, et al., 2013).

**Integration of other Theories into UTAUT**

The UTAUT is actually a an integration of several other theories to include: Theory of Reasoned Action (TRA), the Theory of Planned Behavior (TPB), the Innovation Diffusion Theory (IDT), the Technology Acceptance Model (TAM), the Motivational Model, the model of Personal Computer Utilization (PCU), and the Social Cognitive Theory (SCT) and uses behavioral intention as a predictor as a predictor of technology use behavior.

**TRA**. The Theory of Reasoned Action proposed by Fishbein and Ajzen (1975) attempts to explain and predict the people’s behavior in a specific situation. According to TRA, a person’s actual behavior is driven by the intention to perform the behavior. Individual’s attitude toward the behavior and subjective norms are the ‘loading factors’ toward behavioral intention. Attitude is a person’s positive or negative feeling, and tendency towards an idea, behavior. Subjective norm is defined as an individual's perception of whether people important to the individual think the behavior should be performed. The Figure1 and the associate Table1 below give us a more wide view.

**TPB.** Ajzen (1991) posited the Theory of Planned Behavior to suggest that intention is an immediate predictor of behavior. A behavioral belief (i.e., a specific behavior lead to a specific outcome), weighted by the evaluated desirability of this outcome forms an attitude (Ajzen 1991, p. 188), defines PBC as “the perceived easy or difficulty of performing the behavior”. TPB views the control that people have over their behavior as lying on a continuum from behaviors that are easily performed to those requiring considerable effort, resources, etc.

**IDT.** Innovation Diffusion Theory by Rogers (1995) is a framework to make predictions for the time period that is necessary for a technology to be accepted and is a set of four basic elements: the innovation, the time, the communication process and the social system. Constructs are the characteristics of the new technology, the communication networks and the characteristics of the adopters.

**TAM**. Technology acceptance model (Davis, 1989; Davis, Bagozzi & Warshaw, 1989) was adapted from the Theory of Reasoned Action . Maybe the most well-known and widely accepted and cited model is the technology acceptance model (TAM). Davis (1985; 1989) developed the TAM to explain the computer usage and acceptance of information technology. As Money & Turner (2004) notice, the Institute for Scientific Information Social Science Citation indexed more than 300 journal citations of the initial TAM paper published by Davis et al. (1989).

**Variables Affecting the Adoption of IoT**

This study is based on the UTAUT theory that hypothesizes the adoption of IoT, such as the Smartwatch, is based on five variables – user’s perceptions of usefulness (PE), effort expectancy (EE). i.e., ease of use, social influence (SI), and facilitating conditions (FC) (Venkatesh et al., 2003). Venkatesh et al (2011) later added a fifth factor trust (T). The UTAUT adds moderating factors of gender, age, experience, and voluntariness of use (as depicted in Figure 1— UTAUT Model).

**Review of Core Literature**

Core literature is commonly regarded as the literature within the field of study. (Capella University, 2019). The following literature discusses the background to the problem in the adoption of technology and the particular variables affecting the adoption of technology analyzed in this study.

**Background of the Problem**

The rapidly advancing field of Internet of technology (IoT) has extraordinary potential but carries with it many issues that may deleteriously affect user standardization, scalability, privacy, safety, and especially security (Atzori et al., 2010). Researchers have discovered that users frequently minimize this concern of security in favor of convenience and ease of use of the technology. Furthermore, research indicates that users expect ownership and security of their smart devices and data lost (Bandyopadhyay and Sen, 2011),

Atzori et al. (2010) said that adoption of the technology would be slowed down if the security issues were not resolved. The combination of remote devices with weak control and handling make the IoT defenseless against security issues (Atzori et al., 2010). Security issues of the IoT include privacy, confidentiality, and accessibility (Ning, Liu, and Yang, 2013). At the point when IoT data travel through public networks and systems, it is vulnerable to denial of service and man in the middle attacks (Hurlburt, Voas, and Miller, 2012). Another example is that the utilization of RFID (Radio Frequency Identification) labels in the healthcare industry is normal; however, there are not huge security and privacy issues that need to be resolved (Han, Chu, and Luo, 2011). If personnel data of patients will be leaked to unauthorized personnel than it might lead to dangerous situation for the relative hospital.

Researchers have discovered that users exchange security and privacy for the sake of convenience and comfort in use of devices (Bojanova et al., 2014). As the technology is still growing and developing, it is the ideal opportunity to study the affect and changes desired regarding customer awareness and IoT adoption constraints. As Dlodlo et al. (2012) put it; security remains an important domain for future research regarding IoT.

Some researchers have discovered that users exchange security and privacy for the sake of convenience and comfort in use of devices (Bojanova et al., 2014). With the collection and leakage of confidential data, for example, personal health information, personally identifiable information and other private data, the IoT can possibly hurt users more than encourage them. Therefore, the suitability of this analysis as the Internet of Things is growing cannot be neglected.

By better understanding the elements driving adoption of the IoT, including security, cost, and quality awareness, changes might be made sooner, to increase the adoption rate of the technology and prevent delays in adoption. Since the technology is as still growing and developing, this is the ideal opportunity to affect changes.

From a business and security perspective, the topic is relevant to IoT vendors, service suppliers, and business managers as they struggle to offer IoT items to customers. Atzori et al. (2010) said that few technology and social issues, including "trust, protection, and security" should be sorted out before IoT will be "broadly acknowledged" (p. 2788).

**The Internet of Things (IoT) and Smart Technology**

The expression "Internet of Things" was introduced in 1999 in a MIT presentation by Kevin Ashton (Xu, 2012, p. 701). IoT and Smart Technology are almost synonymous and refer to the collection of interconnected devices using internet technologies. Some examples of IoT/Smart Technology include Alexa, Nike Fuelband, Google Glass, Fitbit, Apple HomePod, Nest Secure Alarm and Google Assistant.

An important feature of the IoT is the potential for smart devices, communicating with different devices, to give significant data and utility to their human users (Dlodlo, Foko, Mvelase, and Mathaba, 2012). Likewise, as the old technologies before it, the IoT may grow more than anybody can predict as of now. Despite the fact that the IoT technology indicates huge potential, there are numerous security issues with the IoT, which may affect its acceptance and adoption by the users (Atzori, Iera, and Morabito, 2010). Eventually, the IoT will empower the independent connectivity of those devices, without human interaction (Dlodlo et al., 2012).

The Internet of Things includes the two ideas of connectedness and individual objects (Atzori et al., 2010). This combination of wirelessly connected devices brings both extraordinary promise and threats. As Atzori et al. (2010) proceeded with the double impression of the term has prompted numerous perspectives on the utilization of the technology. Some have seen the technology from the network point of view, others from the device level, yet others look for a semantic based understanding, trying to apply domain based context of the technology. All perspectives might be correct; as Dlodlo et al. (2012) put it, the IoT will allow the independent and autonomous connection and interaction of the smart devices, developing semantic position, without user interaction.

The IoT is a subset of what will be known as the "Internet of Everything", which is a subset of what will end up known as the "Internet of Anything". Delic (2015) argued that the IoT is particularly the third wave of the Internet, the initial wave being the internet with websites. The second wave is the portable age of internet technology where devices like smartphones helped in establishment of a more socially connected Internet. At last, the third wave is described by Delic as the combination of customer, organizational and home systems into the Internet of Things. Although, there are numerous issues to be resolved before the acknowledgment of that idea, including security, cost and quality (Atzori et al., 2010). In addition, Atzori et al. (2010) said that adoption of the technology would be slowed down if the security issues were not resolved. The combination of remote devices with weak control and handling make the IoT defenseless against security issues (Atzori et al., 2010). Security issues of the IoT include privacy, confidentiality, and accessibility (Ning, Liu, and Yang, 2013). At the point when IoT data travel through public networks and systems, it is vulnerable to denial of service and man in the middle attacks (Hurlburt, Voas, and Miller, 2012). Another example is that the utilization of RFID labels in the healthcare industry is normal; however, there are not huge security and privacy issues that need to be resolved (Han, Chu, and Luo, 2011). If personnel data of patients will be leaked to unauthorized personnel than it might lead to dangerous situation for the relative hospital.

The significance of the IoT is advancing and developing. As Bojanova et al. (2014) put it, the IoT is only a subset of what will be known as the "Internet of Everything", which is a subset of what will be known as the "Internet of Anything" (p. 72). There are also numerous issues to be settled before the acknowledgment of that impression, including security (Atzori et al., 2010).

**Review of the Practitioner Literature**

Following is a review of the practitioner literature organized to present a detailed explanation of the IoT technology and its current state to include examples of Smart Technology, architecture, concerns, threats, and practical issues.

**Applications of the IoT/Smart Technology**

Today, smart things are advertised toward buyers, similar like smart homes, smart workplaces, smartphones, smart network and smart cities (Xu, 2012). Other than the obvious publicity, there are genuine smart services being provided for the advantage of humans. Personal devices as of now exist for the utilization of assisted living. Wearable devices take into consideration the observing of crucial data and developments of senior and other powerless populations (Bandyopadhyay and Sen, 2011).

**Smart Things**

“Smart” technology today pervades all lives in many ways. Following are only a few examples.

**Smartphones.** From multiple points of view, smartphones began the push toward the IoT. By connecting users to the Internet, and giving data at fingertips, the phones changed their lives and the world. Users are no longer attached to classrooms, portable learning has set off and permits "learning whenever, anyplace" (Abu-Al-Aish and Love, 2013, p. 83). As another example, RFID empowered smartphones are presently being examined as substitutes for conventional passports and drivers licenses (Dlodlo et al., 2012). Frequently, through portable applications, other sorts of smart devices are controlled.

**Smart clothing.** Clothing manufacturers are starting to interface dress to the internet. Very soon, users will have the capacity to identify the physical location of a lost coat. Players will have the capacity to screen their temperature during exercises. Installed with sensors for heart rate, clothing will soon provide capabilities like monitoring of weight loss activities. The accessibility of data, for the duration of the day will the wearer to modify their exercises and pick up a superior knowledge to the relationship of activity to their fitness (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

Furthermore, pharmacist are talking about the possibility to screen physical action of patients, with the utilization of smart cloths and other wearable devices, to introduce better health. Researchers are even talking about the possibility to bind cloths with solar threads for power transmission of information. Progressively, the line amongst design and utility will be concealed. Smart clothing falls into the more extensive classification of wearable devices, connected with the Internet. Researchers are planning smart fixes that resemble customary band assistants, however pack sensors to screen glucose levels, potassium levels, and in the long run full metabolic evaluations (Swan, 2012). Formally, smart gloves have been produced that have sensors for temperature, movement, and light detecting: which might be utilized as a part of remote medical and manufacturing situations (Nayyar and Puri, 2016). Smart shoes have provided facilities like the tracking of steps every day and real time information. As can be seen, in the event that it can be worn, it will be associated and utilized as a part of unexpected applications.

This level of technology is changing the idea of human computer interface (HCI), whereby these devices don't regularly have a screen or keypad, the data is posted online or on a multipurpose application. The issue is when sensitive and private data is gathered alongside the usual data. One such case of this over-reach is, when personal fitness devices are observed for evening time activities to derive sexual tendencies (Aditya, Bhattacharjee, Druschel, Erdélyi, and Lentz, 2015). A few applications exist that are intended to advance healthcare and reproductive details (Lupton, 2015). The consequences of having that data put away in the phone and cloud networks are still to be completely figured out.

**Smart Appliances.** Quite a few smart machines have been introduced lately. There are smart TVs that know about user browsing habits and offer access to applications through the TV, obscuring the line between passive entertainment and active utilization of technologies (A. Venkatesh, 2008). Furthermore, there are smart kitchen appliances that know of the levels of nourishment details of the food and help users with health impacts of the food items. (Blasco, Marco, Casas, Cirujano, and Picking, 2014).

**Smart homes.** Home appliances are progressively interconnected, sharing valuable information, to enhance power saving, comfort levels and security. The home clock might be utilized to modify the temperature of the home, further, the alarm system might be utilized to identify movement and turn on lighting and tune the stereo to the owner's favorite channel. Furthermore, users may change their home temperature or other environmental controls through a web and user interface. With the appearance of smart walls and floors, the house is rapidly being changed into a complete user-friendly environment.

**Smart buildings.** Other than smart homes, other type of buildings are also getting smart. From computerized heating and cooling systems, to automated light frameworks in whole building, the buildings are ending up more power effective, with the help of interconnected sensors inserted in the building structures (Atzori et al., 2010). Residents are no more underlying occupants of building; however, their preferences are currently used to transform the once static place of business into an interactive and intelligent workplace. To an ever increasing extent, the line between technology and physical structures is being obscured. The idea of utilizing a building is changing too, though occupants are now just users.

**Smart grids.** Electrical grids are presently connected in unexpected ways. This network takes into account more prominent efficiencies and following of power saving methods. Presently, homes have smart meters, which record power utilization stats, as well as time of day insights, which might be used to power and electricity in a controlled fashion amid high rates of consumption. Customers may run a specific application, for example, charging a vehicle, during the evening, when the cost of power is less expensive (Hahn and Govindarasu, 2011). Furthermore, power might be shared from alternate energy sources, for example, sources like solar powered. In a few circumstances, users may offer power back to the grid, which is in access of user’s requirement. As pointed out, about smart network and grid technology, communication methods are mostly utilized to achieve high availability.

**Smart cities.** Smart cities incorporate a level of automation, which was just imagined previously. After water, power, and gas, smart city framework is viewed as the most important infrastructure (Kang-juan and Liu-qing, 2012). Parking meters will take into consideration coinless activity and the identification of accessible spaces, over the city.

Furthermore, connection points might be connected, with the goal that traffic lights are poised to course traffic in an effective way. Researchers have imagined a context where "smart cars" collaborate with "smart roads" to enable the user to have numerous in-trip choices, for example, route determination, parking bookings, lane adjustments and automated toll handling (Varaiya, 1993, p. 1). With this more noteworthy level of access to technology, comes an expanded requirement for security. In the event that an intruder picks up control of a city's infrastructure, gridlock may result.

**Smart transportation systems.** The transportation business is established for proficiency. Technologies, for example, RFID are now utilized today for the real time tracking of goods, providing more noteworthy efficiencies (Bandyopadhyay and Sen, 2011). Tomorrow, the IoT will empower the tracking of goods from generation to retail to checkout at the store, automatically. This technology, combined with smart home technology will empower the delivery of goods to the home, when required, automatically. Nevertheless, with the majority of this automated processes comes the threat of loss of privacy. The tracking of personal information, socioeconomics, shopping habits, and consumer’s physical location is genuine threat to the security. Customers are mostly unaware of the privacy threats, until the point that it is past the point of no return.

**Smart automobiles.** The IoT is changing the car business. Amid assembling, sensors are utilized on parts to track their origin, installation, and repairing (Bandyopadhyay and Sen, 2011). Furthermore, sensors are utilized as a part auto industry, from sensors in tires transmitting weight analysis with respect to other vehicles. Wireless technologies, for example, Bluetooth and RFID have been basic in the use of car technology, as space for wiring is at a premium. Utilizing Bluetooth, users may presently communicate with different drivers (Dlodlo et al., 2012). Further, the user’s smartphone might be utilized for sending addresses for route and tracking, tire pressure and maintenance statistics. However, these systems are equally vulnerable to threats as other technologies, so proper measures are required to secure these systems. Although, in 2015, a few programmers displayed the vulnerability of smart cars being exploited trough internet.

**Smart medical and health care.** The IoT will offer remote human services, whereby patients and suppliers are no longer tied physically. RFID and different wireless technologies will enable the tracking, monitoring and delivery of medical facilities for the patient (Bandyopadhyay and Sen, 2011). Possibly, healthcare services can be given to the patient without much of human interaction. The physical location of doctors, specialists and staff might be tracked in real-time to provide efficient and quick services to the patients (Dlodlo et al., 2012). The privacy constraints are critical, however the security concerns might be considerably more so. Now, the IoT will be able to save life.

**Smart cost-control.**  Companies in sectors such as education, health, finance, agriculture, retail and transport, will demand more this type of solutions because they seek to have better control of their business. Although 2017 was a year of experimentation in terms of IoT for firms, we will see that in 2018 many of them will specialize in handling IoT solutions and will be more participatory in designing them to solve their needs. According to the Company's Innovation Index, three out of ten companies have already implemented an IoT solution. While among the organizations that still do not, five out of ten plan to do so in the next 12 months. The analysis also indicates that companies invested mainly in IoT solutions for the monitoring of fleets, smart buildings and manufacturing operations.

Organizations can generate new business opportunities , improve their operational and productive processes by analyzing the volume, variety and speed of the data produced, while at the same time having greater visibility and control of their business, which in turn allows them to Anticipate problems and make decisions quickly. It is expected that in 2018, we will also see how companies will implement their business processes in IoT, with the aim of improving their customer services, translating into an impulse in the processing and analysis of data to reduce their costs.

**Smart quality of service (QoS).** Analyst IDC says that the global Internet of Things (IoT) market will go from 655 billion dollars in 2014 to 1.7 billion dollars in 2020. Likewise, companies such as Cisco and Ericsson estimate that the number of connected devices will increase until reaching 50,000 million during the same period.

Given this scenario, it is logical to think that organizations from all sectors of activity are considering how to transform their business processes and find the best ways to take advantage of the opportunities provided by IoT.

This reality supposes to accept a radical transformation both in the conception and in the development of the businesses, since now, independently of its object, all will have as fundamental base a technological component. This fact is not trivial. It means that the main channel through which a product or service will be delivered, or through which support or maintenance will be provided, will be a telecommunications network. If this network fails, there will simply be no business.

**Microcontrollers.** As things get smaller and smaller in size, so does the technology that drives them. Microcontrollers are the installed chips that drive the things of the IoT and allow distributed management and independence (Dlodlo et al., 2012). Size, memory, processing prowess, and power requisites end up becoming critical while examining the usage of security systems. A few things will have constrained power and computing resources. Power sources may incorporate solar based, sound, radio frequency, and different sources like electricity (Bandyopadhyay and Sen, 2011). Whenever control sources are not accessible, things may need to exploit different things to convey data. The absence of power and computing assets may require a few things to deliver messages (Bandyopadhyay and Sen, 2011). The shortage of power source affects security. Services, for example, encryption and verification take a certain level of power and assets that may not be accessible for the device, resultantly the security of the whole system will be compromised.

**Computing and networking.** Communication for IoT devices is essential for the usual operations. As devices of different insight and specifications are associated, networking and communication issues, for example, transport, flexibility, discovery of other devices, and protocol and standardized methods become necessary (Bandyopadhyay and Sen, 2011). Up until this point, radio frequency ID (RFID) is "the foundation" of the IoT, especially in manufacturing (Bi, Xu, and Wang, 2014, p. 1541). RFID sensors come in two variants, active and passive sensors. Active sensors contain batteries and may effectively start interchanges with other devices. While, passive sensors don't contain batteries and must gather their power capacity from a transmitting close-by power-source (Atzori et al., 2010). In spite of the fact that many RFID researches have concentrated on privacy issues and other important components of security, for example, data altering and tampering remain a concern. One proposed type of temper identification method, utilizing computerized watermarks to help address this issue. The absence of research on fixing other different security perspectives remain an issue.

Future IoT network systems are imagined to hold sensors that are to be deployed in an ad-hoc manner, therefore, more security issues are supposed to arise in these networks. (Lacuesta, Palacios-Navarro, Cetina, Peñalver, and Lloret, 2012). In this situation, the sensors will connect and communicate with each other without need of human interaction.

### Cellular network. Cellular networks and systems, including GPRS, GSM, 3G, and 4G are utilized for long run communication (Z. Chen, Xia, Huang, Bu, and Wang, 2013). Long range communication is valuable, as sensors might be deployed quite away from their user or associated peers. Uses of this type of interchanges include remotely associated structures, cars, and smart phones.

WiFi. The IEEE 802.11 protocol has been set up for a very long while now and fills in as the standard for medium range communication services, in spite of its moderately high power requirements (Jayakumar et al., 2014). The general idea of WiFi has moved it to the front of the list of wireless technologies for the IoT devices. WiFi has experienced an advancement of updates, replacing the old wireless technologies that had many security issues; however, proper care must be given while designing IoT, to choose the more secure options available. Disappointingly, users know little about how to design a secure WiFi network, therefore depend upon the manufacturers and default installation setting.

**Zigbee.** The IEEE 802.15.4 protocol is the standard for low power, low complication, and short-range communication, normally for a couple of meters (Sheng et al., 2013). A few protocols have been based upon the 802.15.4 standard, including Zigbee, which is developing as a most valued convention for IoT devices because of its low power requirements (Z. Chen et al., 2013). Zigbee takes into consideration communication methods that not only define whom to communicate with but also provides details regarding how to communicate. (Asensio, Marco, Blasco, and Casas, 2014). One of the issues with Zigbee and other sensor level protocols is the way that they work at layer 2 and in this way cannot communicate directly with other Internet devices, which work at layer 3 and higher (Jayakumar et al., 2014).

**Bluetooth (LE).** The venerable Bluetooth protocol, which is utilized to such an extent as WiFi, has experienced an overhaul, and the Bluetooth low energy (LE) protocol has risen as a more feasible option. Bluetooth LE is in some cases introduced as "Bluetooth smart" because of its capacity to save power, yet be backward compatible (Jayakumar et al., 2014, p. 377). Similarly, as with Zigbee, the Bluetooth protocol can't communicate with the Internet. In this manner, Zigbee and Bluetooth are regularly utilized as a part of conjunction with a gateway device to communicated with devices from higher level networks.

**6LoWPAN.** The Internet Protocol version 6 (IPv6) over low power wireless personal area networks (6LoWPAN) standard is rising as the approach to apply IPv6 over 802.15.4 systems. One of the difficulties that 6LoWPAN faces is the moderately low packet size limitations of 802.15.4 systems (127 byte frame sizes) (Sheng et al., 2013). This is especially an issue for IPv6, which has a Maximum Transmission Unit (MTU) of 1280 bytes. As Sheng et al. clarified, the 6LoWPAN supplies a thin layer, appropriate over the data link layer, to fragment and reassemble the IPv6 packets in a proficient way (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

Sensors

Sensors are what make the IoT something beyond the Internet 2.0. Sensors have the capacity to detect the system condition and process information independently. Whenever an RFID sensor in a car goes under a roadway toll meter, the user does not have to interact with the system; it simply happens automatically (Gao and Bai, 2014). In 2008, the number of sensors connected with the Internet surpassed the quantity of humans on the planet; by 2020, the number is supposed to exceed 50 billion (Swan, 2012).

What makes the IoT extraordinary is the capacity to associates devices, as well as to empower devices to act independently. Sensors, won't just accumulate data, yet will make choices on what to do with that new learning. Researchers have argued that sensors will work in two modes (or circles), information gathering and sensing (Zaslavsky and Jayaraman, 2015). They went ahead to present that this discovery procedure would empower devices to acquire information utilizing reasoning strategies.

In the long run, sensors in smart devices and vehicles will empower the alarm clock of a business official to detect the morning meeting has been delayed for 30 minutes and allow the official to rest more, and advise the coffer maker and car to sleep for 30 more minutes as well (Hurlburt et al., 2012). The security propositions are striking. A busted timetable is the least thing that could happen. Therefore, IoT is the connecting of defenseless devices that is leaving users powerless in new and unanticipated ways.

**Architecture of the IoT**

**Edge layer.** The IoT devices frequently communicate at layer 2 of the ISO communication standard model. In this way, they convey in a shared mode and are frequently limited from Internet (Bandyopadhyay and Sen, 2011). There are special cases like at times various communication ways are given, as in the use of smart grid technologies, which utilize long-range communication mechanisms.

**Access Gateway layer**. The access gateway layer is intended to empower sensors to convey outside their sensor level system, to higher-level systems, for example, the Internet (Bandyopadhyay and Sen, 2011). At this layer, the gadget may take data accumulated over Bluetooth, Zigbee and transmit that data by means of intermediate and long-range communications, for example, Global System for Mobile communication (GSM) or WiFi (Asensio et al., 2014). This layer is basic for security. To be specific, an attacker should not have the capacity to establish an unauthorized connection.

**Middleware layer.** The middleware layer is critical to give an extension between the lower hardware communication layers and the user level applications. The middleware layer gives a layer of deliberation whereby the designer does not have to think about the lower layers of communication and may execute more high level constructs, for example, service oriented architecture (SOA), which takes into consideration software reuse and is getting to be widespread in IoT plan (Atzori et al., 2010).

The middleware layer considers device abstraction too. Researchers have built up an IoT Management Platform, which can be utilized to oversee devices and give device level data and in addition behavioral related information of devices (Elkhodr, Shahrestani, and Cheung, 2016a). Furthermore, there are new platforms being introduced particularly for machine-to-machine (M2M) connection. ThingWorx is an IoT platform, including merger capacities that empower the connection of things (Nakhuva and Champaneria, 2015). By defining building blocks, the middleware layer is basic for development of the IoT.

**Application layer.** With the goal for things to be smart, applications are expected to bring usefulness and convenience (Bandyopadhyay and Sen, 2011). Regularly utilizing online protocols, applications communicate on behalf of users (Atzori et al., 2010). Just because online protocols are utilized, does not imply that the application has a conventional human user interface; mostly they do not. The combination of the edge, gateway, middleware, and application layers permit IoT devices to communicate and become helpful in a several applications.

**Security and Identity Links**

With personal use come personal level risks and threats. To worsen the situation, the things of the IoT regularly do not have a user interface, making it impossible for users to control security settings (Atzori et al., 2010). According to Bandyopadhyay and Sen (2011), users regularly compromise security for the sake of a service.

In the field of RFID (Radio Frequency Identificaiton), there remain issues of data integrity and data leakage. Security of important data gathered by IoT devices is an issue that is pointed out by many researchers (Hurlburt et al., 2012). Others have pointed out towards the wireless mode of communication used by the IoT devices, which makes them vulnerable to even more attacks. Furthermore, unless and until all these security risks associated with the IoT technology will be resolved, acceptance and adoption of this technology will not significantly increase (Atzori et al., 2010). What is not important is the particular effect of security issues and other "drivers of user’s acceptance of the IoT technology" (Gao and Bai, 2014, p. 224). In this manner, the issue this research addresses is the negative effect security issues have on acceptance of the IoT technology (Atzori et al., 2010). The subsequent research will help IoT vendors, service suppliers, and business managers to increase technology adoption.

**General Security Concerns of the IoT**

Data security can be summed up as the safeguarding of the integrity, confidentiality and availability of data and data assets (resources) (Calder and Watkins, 2012). In a personal setting, the individual is in charge of their security. While in a business setting, the obligation of an association's data security depends upon the higher management authority, specifically related to IT administration (Calder and Watkins, 2012). These may include Chief Executive Officers (CEO)'s, Chief Information Officers (CIO)'s, or Chief Information Security Officers (CISO)s. A viable method to oversee data security threats is to perform risk assessment (Calder and Watkins, 2012).

**Assets.** The information security risk assessment begins with an understanding of assets that fall within the scope of the project (Calder and Watkins, 2012). As proposed in (Hogben and Dekker, 2010), future threats in a versatile domain may influence diverse resources, such as "personal data; corporate classified data; financial resources information; device and service accessibility and functionality; individual and political image" (as referred to by La Polla, Martinelli, and Sgandurra, 2013, p. 450). The estimation of assets of an organization manage the level of security required. Next, it is useful to consider the threats to the given resources of an organization.

**Vulnerabilities.** There is a sharp rise in the quantity of vulnerabilities in operation systems as of late. Furthermore, other IoT platforms are also defenseless. Vulnerabilities are shortcomings in a network, system or applications that leave them exposed to attacks (Calder and Watkins, 2012). It is through the vulnerabilities that threats exploit an IT asset. There is an immediate connection between vulnerabilities and effect on the security of the system (Calder and Watkins, 2012).

Consequently, if there were no vulnerabilities, there would be no risks to the IT systems. Then again, if there are more weaknesses and vulnerabilities, there will be more influence to the security of the IT assets. At the point when users carry their own devices into the workplace, they carry vulnerabilities with them. A few devices might be updated with the latest upgrades and fixes for security issues (vulnerabilities), others may remain vulnerable, and therefore making the whole system vulnerable (Miller, Voas, and Hurlburt, 2012). It might be said, the organization is getting the security posture of the users, not the other way around. Those security issues tend to transfer into the whole network and the systems and confidential data might get leaked (Miller et al., 2012). This difficulty displays a genuine issue for IT administrators today, and it is getting exceedingly terrible, with time.

**Current threats.** Threats are things that can turn out badly and represent a risk to an asset (Calder and Watkins, 2012). Milligan and Hutcheson (2007) put it best, as they talk about risks, threats also, countermeasures for smartphones. They expressed that a few cases of threats include: "data leakage coming about because of device loss; unexpected disclosure of data; attacks on decommissioned devices; phishing attacks; spyware attacks; network spoofing attacks; reconnaissance attacks; dialerware attacks; money related malware attacks; denial of service attacks". Threats might be moderated by security controls, which go about as counterbalances against threats (Calder and Watkins, 2012). Threats are not static; they have a tendency to advance after some time. Threats have the ability to exploit the organizations data resources and assets (Calder and Watkins, 2012). Conventional threats incorporate outside and insider attackers, frameworks and technology failures (Cebula and Young, 2010). With regards to the human threats, Cebula and Young (2010) portrayed three sub-classes: accidental, deliberate, and inaction. Of these, the deliberate type is of mostly concerned in this study. Activities, for example, sabotage fraud and vandalism might be described and recognized utilizing conventional digital security protections (as refered to by La Polla, Martinelli, and Sgandurra, 2013).

**Future threats.** The future cybercriminals will progressively concentrate on smart devices. Gostev (2011) maintains this reality as he states attackers: "will concentrate on iPhone and Android devices" (as referred to by La Polla et al., 2013, p. 449). As described by Machol (1976), while probing the "Sutton Effect", offenders will go where the cash is (La Polla et al., 2013, p. 449).

**Consequences of Threats**

There are many potential consequences of threats.

**Compromise.** The most noticeably appalling thing that can happen to an IoT device is system compromise. At the point when an attacker can take control of an IoT device, they may insert their own malicious applications and utilize the device in dangerous ways. By then, the user can never again trust the system as the system is presently compromised and under the control of the attacker, not the user. System compromise is frequently the initial phase in further misuse. The accompanying threats are simple, once system has been compromised (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Privilege escalation.** Once an attacker accesses a system, the attacker will attempt escalation techniques to get more privileges in the system. If attacker had user level access, he would attempt to gain administrator level assess to take complete control of the network and systems (Whitehouse, 2014). Frequently an attacker must take vulnerable configurations and settings of the system and network and use them to exploit the system and gain complete access of the system (as refered to by La Polla, Martinelli, and Sgandurra, 2013).

**Impersonation.** Once an attacker has acquired access of the whole system and network, they will try to impersonate as different users already present in the network, keeping in mind the end goal to avoid detection by antivirus or firewalls. Impersonation has another risk to the user, that of non-repudiation (Airehrour, Gutierrez, and Ray, 2016). Specifically, if the attacker performs some malicious activity on the network using some legit users behalf, it would be difficult repudiate those actions.

**Persistence.** Once an attacker has experienced the process of gaining access to the system, escalated privileges and impersonation, in next phase the attacker would try to gain persistence over the network (as referred to by La Polla, Martinelli, and Sgandurra, 2013). Furthermore, to gain persistence, the attackers normally modify the system configurations. Moreover, the attacker will deploy backdoors in the network so that the attacker can access the network later on. The attacker does not want to lose that advantaged position in the system. Along these lines, the attacker will make a huge effort to ensure persistence over the network (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Data discovery.** Since the attacker has ensured their access, the attacker will attempt to gain as useful data from the network and systems. Confidential and important data for the attacker might include Personally Identifiable Information (PII) or Personal Health Information (PHI), and financial information. Attackers will scour over all the files on the servers, and search for delicate and useful information. Once identified, attackers will transfer the data from the network to own storage locations (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Data tampering .** Data does not always need to be stolen to effect users. Sometimes, tampering up the data can cause tragic impacts. A security researcher found and unveiled a vulnerability in remotely connected insulin pumps that may enable a dose of insulin to be changed by an attacker, possibly hurting the patient, without them knowing what happened. Envision for a minute, how would one inspect such an event, whose blame would it be? (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Man in the middle.** It ought to be noticed that data leakage and data tampering should be mitigated from the IoT device itself, if the attacker gained access to sensitive information traveling within in the network and between different devices. Attacks that are launched to compromise and gain access to the communication channel between two devices are referred as man in the middle attacks, whereby an attacker catches delicate communications and alters the data in course to the other user (Atzori et al., 2010).

**Denial of service.** At the point when all other attacks come up short, an attacker may try to deny the user access to the server or data. A denial of service attack does that and tries to block a legit user from accessing services (Airehrour et al., 2016). Since this sort of attack has the undeniable potential to be identified quickly, it is frequently utilized as just a final option by the attackers.

**Specific Security Issues of the IoT**

The security issues of the IoT are nothing new, as it is just the latest example of the mindset of technology developers regarding security being an afterthought (Mansfield-Devine, 2016). There are, however, some new concerns applicable to the IoT technology:

**Embedded security issues.** The way that the IoT depends on embedded technology causes some interesting security challenges. Regularly security issues emerge at various layers of hardware equipment, operating systems, and applications. Along these lines, security (or insecurity) of one layer may influence the security of another layer. To make matters worse, the manufacturers of devices are working on thin edges and frequently under impossible requirements. One method is to allow the signing of code, from the manufacturer, into the application (Mansfield-Devine, 2016).

**Wireless security issues.** IoT devices experience the same indistinguishable security vulnerabilities from different technologies. In any case, a few issues might be exacerbated. Since there is no user interface on numerous IoT devices, how is a user expected to safely design the wireless settings? To make matters more terrible, because of interoperability and power constraints, it might difficult to execute encryption to the communication between devices (Bandyopadhyay and Sen, 2011). In this manner, wireless protocols might be used without assurance of the confidentiality and integrity of the data and without the user knowing about these constraints (as refered to by La Polla, Martinelli, and Sgandurra, 2013).

**Monitoring Challenges**

Monitoring of the IoT devices is a testing task. One of the primary reasons is the need of a user interface. Furthermore, some communication is performed at layer 2, which does not allow directing messages outside the sensor network. In this way, once an IoT device is endangered, there are little methods to recognize its unauthorized access. A few researchers have found anti-analysis and analysis-evasion techniques used in malwares, making the malware resistant to detection. These conditions all prompt towards a troublesome area for security providers and will remain a territory needing further research for quite a while (as referred to by La Polla, Martinelli, and Sgandurra (2013)).

**Big data problem.** The enormous data gathered and handled by scattered sensors displays a major data issue, as far as security. To be specific, the sheer number of end devices will overpower conventional security checking advancements. A few researchers have proposed, the existing Security Information Event Management (SIEM) apparatuses might be refined to utilize correlation and regression analysis to go through the mountains of data and detect if any intrusion takes place. Unlike the existing SIEM, which depend on correlation, the researchers propose utilizing regression to possibly finding new threats (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

Another Big Data issue to consider is that of the gathering of user related information, and the privacy ramifications of that. In 2015, the Whitehouse released a report that illustrated the threats of gathering large amount of data from users and the requirement for a new "responsible use system" which puts an emphasis on the ethical constraints of data handling (as refered to in Federal Trade Commission, 2015, p. 25).

**Secure framework designs.** Progressively, researchers are creating secure structures for IoT devices to work. Researchers recommended an end to the usage of traditional security framework that has been used in IoT technology. Furthermore, it was recommended to incorporate transport security, physical security, cryptography, and application security. Rather, it was recommended to adopt a completely new framework, which will be a lightweight, with a digital forensics module embedded, a inter device communication module, and a system based user interface. Adopting an alternate strategy, Chen et al. (2014) proposed a data fusion structure to protect IoT systems. Utilizing strategies customarily found in the biological field, Ding et al. (2013) proposed using the independent capability of the IoT devices and enable them to self-arrange to shield against attacks. Some have proposed secure verification systems utilizing security certificates as the way to fixing the IoT security issues. In any case, as Lin et al. (2015) pointed that special care must be given when creating key-based verification and authentication modules for fear that an attacker can exploit weak design and bypass the authentication process of the system. Others, for example, Harrop and Matteson (2014) propose that more exertion ought to be put in the home systems that IoT devices reside in. The smart grid system ought to be secured in the first place, before including more smart sensors to the system. While, Tan et al. (2006) argued for the mix of all security models, through a semantic approach, utilizing the basic decision-making capabilities of the independent nodes. Despite the fact that there are numerous research available on improving the security of IoT, one thing is without a doubt; all agree that it is mandatory to be achieved (as refered to by La Polla, Martinelli, and Sgandurra, 2013).

**Autonomous computing.** The autonomy of things may prompt less autonomy of humans, which is an ethical issue. Humans are hard wired to take decisions and have complete control over their environment (Wakunuma and Stahl, 2014). In case of IoT technology, most of those decisions are made for the human, Brehm's reactance theory expresses that less choices prompt less control prospects (as referred to in Wakunuma and Stahl, 2014). Furthermore, when a device takes a decision for a human, a feeling of reliance is built up and the human is less free. There is another viewpoint to consider here. Some researchers have expressed that IoT devices might be thought of as "creatures" and subsequently be sorted out into communities and societies (Karimova and Shirkhanbeik, 2015, p. 1). Obviously, the ethical issues should be tended to before the IoT achieves its maximum capacity.

**Privacy.** A frequently ignored part of the IoT is the privacy concerns of the technology. The sensitivity of privacy concerns differs universally. What happens when a user leaves an organization and there is private data alongside organization data on an IoT device? What happens when an organization have access to a user's personal data through an IoT network? It is proposed that an employee is consulted before deployment of the IoT systems and regularly updated about the organizational policies concerning the IoT networks. Concerning security and the IoT, there are two kinds of data. Security of locations related privacy data includes ensuring data of personal location of the users. While, personal data protection includes the insurance of delicate personal data of users (Bandyopadhyay and Sen, 2011). The key factor that makes privacy different is the personal nature of the data. There have been a few instances of worry for personal data tracked on RFID labels, including Passports and tickets. To worsen the situation, the absence of a user interface on numerous IoT devices has resulted into passive utilization of the technology. There is likewise an issue of ownership of data, concerning the IoT (Hurlburt et al., 2012). This passive utilization of technology has caused an unexpected situation, where users are not in any case aware of their personal data being recorded. Given an opportunity, governments, business elements also, attackers alike will discover approaches to collect the immense amount of personal data of users.

**Safety.** Security might be upgraded or impeded with the IoT. IoT technology may navigate numerous enterprises and businesses, including open security (Bandyopadhyay and Sen, 2011). Imagine that a kid is far from home and is lost. Utilizing the services of the IoT, like he might be wearing a little wireless device and can be tracked using that device. On the other hand, think about an attacker, ready to monitor that same kid's location and movements over the Internet, through that same device. The double idea of the technology may introduce different difficulties (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

Medicinal services is another zone where privacy, security, and health constraints meet. The utilization of RFID labels in the medical services industry is normal; anyway, there do not have high security standards implemented in these setups and result into serious security concerns. Further, computerized and connected devices presently hold medical and personal data in medical centers and are utilized for the proficient reservation processes, profiling of patients and better administration of social insurance for the good of patients. Anyhow, it is down to these similar type smart devices that are trusted to ensure the privacy and security of patient data. At the point when leaked to unauthorized people, attacker for illicit means can utilize critical data. Furthermore, if these data are deleted or altered from the servers by the attacker, then the patient might be facing disastrous situation. Despite the fact that the risks are obvious, as Bojanova et al. (2014) explained it, still, people tend to exchange convenience for privacy and security. This is a terrifying idea concerning personal data, yet that is not the main region of concern for the IoT developers. RFID labels are right now used to track all the appointments and developments of treatment process, which becomes essential when settling quality issues, because of a reappointment (Dlodlo et al., 2012). The concerns related to health of the patient are basic ethical issue of the IoT.

**Practical Issues of IoT**

Besides the security, ethical and legal issues of the IoT, there are other factors that are needed to be considered as described following.

**Standardization.** The absence of any standardization in IoT causes a few issues, including security related issues (Atzori et al., 2010). In the event that there is no standard and generally acknowledged convention for communication between devices, then the devices won't be able to safely communicate with each other (Airehrour et al., 2016). Furthermore, quite a few domains of standardization in the IoT require significant improvement. As examined, the 6LoWPAN protocol is an improved and standardized version of the 802.15.4 standard that is still being utilized as a communication standard at the data link (layer 2) to use IPv6 communication in an IoT setting (Sheng et al., 2013). This is critical, given the high number of devices to looking to connect are still using old IPv4 standards and lack spacing. As Sheng clarified, standards are being introduced at each layer. At the network layer (layer 3), IPv6 is turning into the standard that every technology is opting for. At the operating system level, extraordinary steps are being made to standardize on lean, uniquely designed operating systems, without the issues generally found in other cases. These lean, limited stack operating systems are more control proficient and offer help for high-speed communication and applications. At the application (layer 7), the REST convention is developing as a standard (Sheng et al., 2013). Standardization are vital for bi-directional communication and proper working of the IoT technology, and that while meeting security standards (Bandyopadhyay and Sen, 2011). Without standardization, the IoT will not achieve its maximum capacity.

**Fault tolerance.** When working in a resource-starved environment, with less than ideal communication paths, fault tolerance is an important requirement for the IoT technology. Sensors can further be used to help with detecting faults (Atzori et al., 2010). Nevertheless, the fault detection should not itself depended upon. Instead, robust networks, sensors, and control devices should be deployed to operate in remote environments and to further make some decisions independently. Whitehouse (2014) suggested that a three design criteria should be utilized when designing robust systems, the devices should be made secure by default, and each device should be made aware of its own status and the status of the network as well as status of other devices. Furthermore, each device should be able to defend itself from any kind of attack or network outage. In such circumstances, the overall service of IoT would be degrade a little, but it will still persist. Whitehouse (2014) recommended for fault injection testing to be added as major stage of the development process, which will help in achieving of the system to tackle attacks or power outages.

**Interoperability.** Interoperability can be described as the ability of an IoT device to communicate with other devices that exist within the network. The interoperability issue is to enable social cooperation between devices developed by different vendors. Furthermore, these devices might be having different standards being utilized in their development and processing. Interoperability is required for maintaining high levels of security, privacy, and trust of the users and their data (Bandyopadhyay & Sen, 2011). Most of the times interoperability causes devices to move into less than secure states, like a device might not be encrypting the communication (Airehrour et al., 2016). In any case, interoperability issues should not affect the security of a device; instead, it should enhance the security. Standardization is a method to allow for Interoperability, while maintaining protection (Elkhodr, Shahrestani, & Cheung, 2016b).

**Trust.** As an IEEE report put it, “Earn or Give, but Never Assume, Trust” (Arce et al., 2014, p. 9). In that study, it was discussed that most of the times the trust misplaced by the developers and users, so the fundamental security and safety features of the smart devices are compromised. When a trusted server delegates sensitive operations to the client, this relationship depends upon trust between the devices. Another example is supposing that an unauthorized attacker will not access valuable code, present in the client or mobile application, which is also form of a misplaced trust in the operating environment by a mistaken developer. The researchers further elaborated a different model, which checked all the data received from untrusted devices inside and outside the network before utilizing it. However, some researchers discussed, that trust should be established between network connection process and access to the system should only be granted depending on the level of trust (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014). A trust chain is to be developed and network resources are to be granted or denied to the user based on that trust. This idea can be further extended, using certificates to establish trust between two nodes, with no previous knowledge about other devices. Any exploitation of these certificates would be a misplace in trust, as described by Arce et al. (2014).

**Governance challenges of the IoT.** From business management point of view, the IoT faces some unique challenges, and will definitely need a new form of control (Dutton, 2014). While, from security management program viewpoint, the security policies, the training and awareness, the monitoring, and each aspect of IT management will need a change to bring into line with the authenticity of the IoT.

**Security program management.** Security program management is tip of the security management domain. Security program management can be defined as the set of polices, monitoring and training, which allows for the deployment of controls mentioned in information security management model (Y. Chen, Ramamurthy, & Wen, 2015). Any organization’s functional ability to implement the security system will get mature with the passage of time. With the rapid speed the IoT technology is being introduced and implemented in the organization need to answer questions like who is the owner of the IoT system, who will be responsible for the overall security of the IoT system, and who will contacted in case of a system compromise? Answering these question present a major challenge to the security advisors and professional (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Security policies.** The best approach to introduce and implement the security polices will be to begin with a business impact analysis (BIA). For this purpose, a thorough study should be conducted regarding assessment of integrity, confidentiality and availability constraints of the business resources and user security. In case of IoT devices, the traditional interpretations of integrity, confidentiality and may apply, but, new requirements such as power management constraints and resources related constraints must be added (Jayakumar et al., 2014). Furthermore, while describing the encryption mechanism, which will be implemented in all the IoT process and to sensitive data, a resource starved smart device will not be able to use such functionalities.

This initial level BIA analysis will help in attainment of high-level security policy implementation, without going into much details of how to operationalize it. In the next phase, a threat analysis is performed to evaluate which threats are more likely to take place and how they can be mitigated. The threat analysis needs to add mitigation procedures of the aforementioned threats to the IoT devices (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

After threat analysis is complete, a vulnerability assessment will take place, during which all the vulnerabilities of the devices, network and IoT technology will be determined. Eventually, action oriented policy statements will be formed to stop threats from getting access to the valuable assets and devices. These action statements will be deployed to the high level policy frameworks to further optimize the IoT system. By starting with a Business Impact Analysis, including the impact of the IoT devices, polices will be determined to secure the systems and to attain business success.

**Security Education, Training and Awareness (SETA).** Any policy implemented to any technology will not able to achieve desired results unless and until the users of the technology will not be aware about those policies. Security Education, Training and Awareness programs help the users aware of the security policies and their effective use (Y. Chen et al., 2015). Because IoT technology is mostly facing issue of lack of user interfaces forms of the IoT devices, users will require extended level of guidelines to properly use the technology and meet the security demands. An organization will be as strong as its weakest link is weak. Down to challenge of device compromise because of a weak password set by the user, the complete organizational network will be compromised (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014). S ETA programs are used to make the users aware of all the possible threat that they can face and suggested how they can keep themselves and the organizational assets safe from these threats.

**Monitoring of policy.** With education and the awareness, any policy implemented will still fail if it is not properly monitored. The security policies are to be properly monitored for the effectiveness and are supposed to be genuinely enforced to achieve organizational and individual security. Monitoring should take place for all the organizational policies and smart devices, but especially for those devices, that does not share a user interface and usually transmit sensitive data to other devices in the network, and that without the user even knowing it (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014). Furthermore, the users need to be aware about the fact that their devices are being monitored. Studies have shown that a positive relationship between security culture, security policies and user knowledge of policy monitoring helps the organization in achieving better security (Y. Chen et al., 2015, p. 17). While the security capabilities of any organization increase, more monitoring will be required and more efforts will be required from the organization.

**Information security governance of the IoT.** Security program management is only the tactical implementation of an organization’s security governance strategy. However, enterprise management calls for IT management and IT management calls for security management, security management depends upon the security program management for the overall implementation and execution of security policies of the organization. Security programs hold all the policies, training procedure, and monitoring methods to execute proper controls and govern the organizational risks at an appropriate level. Furthermore, the management structure will be dictating what steps should be made and outline for the whole security program will be provided. Since, IoT systems are mostly connected to the business networks, the management strategy include details regarding all the resources. Therefore, the IoT procedures within any organization should be initiated at board level (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014).

**Organizational effect of the IoT on Policy.** While the organizations attempt to accomplish the organizational objectives, the IT projects should be merged with the IoT processes. For the implementation of those projects, the security program should be implemented, updated if required to, and used to achieve successful implementation of the IT project (Asensio, A., Marco, A., Blasco, R., & Casas, R. 2014). Furthermore, if the decision has been made by the organization to utilize the IoT, and to meet the business objectives using IoT technology, then the security program should be implemented for that and should share details regarding impact of that decision as per existing security policies. However, for most of the times, the policies are adjusted to make space for the emerging requirements into the existing implementations (Goguen & Meseguer, 1982).

**Cultural effect of the IoT on policy.** Actions of the users mostly are effected by proper implementation of security strategies and polices. Furthermore, because of the awareness programs introduced by the organizational regarding the monitoring policies, help in establishment of a working environment that eventually improves the overall security of the organization. Moreover, employee behavior and attitude towards the organizational policies, monitoring and training program describes the overall organizational security culture (Y. Chen et al., 2015). That security culture will helps the organization in creating better awareness of threats to the IoT devices. As the security culture of an organization improves, the organizational security becomes less susceptible to all forms of attacks.

**Application of the Literature**

This research is very significant in predicting the choices and needs of customers willing to adopt IoT. It can also be employed as a market study regarding the demand and supply of IoT products. With the increasing number of IoT products in the market, questions regarding the security of user data are also asked, if not answered, in this research. These questions will not only be the topic of future research but they will remain an increasing concern for network security professionals in the coming years. Multinationals such as Apple Inc. understand the potency of this new and emerging field and are thus willing to invest millions of dollars in this field.

The shift of technology from individual electrical components to a network-based system has and will always, prove to be difficult to keep secure. The direction of this research is aimed at understanding the fundamental problems that arise due to the complex connectivity mechanisms that are used, and the scale to which they need to be addressed. This thesis also aims to study the fundamental factors of human decision making involved in accepting or rejecting a new technology.

Awareness campaigns regarding cyber-security need to be run on a governmental level to communicate concerns regarding social engineering attacks. Such attacks can sometimes only be prevented by improving user awareness regarding cyber security. This study will not only help the cyber-security professional in introducing counter measures to attacks but also government officials in combatting flaws in their cyber-security mechanisms.

Nowadays, IoT is not only developing on its own but it also continues to transform other related fields. We have already discussed the expansion of cyber security in the field of IoT. Fields like embedded systems, real-time analytics and commodity sensors have been majorly affected by the recent research in the field of IoT. Several research papers have been published regarding the use of electrical power and electrical systems which argue that the advancements in computational intelligence technologies and IoT can be a big factor in future advancements in the field.

## CHAPTER 3: METHODOLOGY

**Chapter Overview**

This chapter presents a detailed discussion of the research design including data collection, description of the data, data collection instrument and process, description of the statistical analysis and results procedure and interpretation.

### Statement of the Problem, Research Question, and Hypotheses

The rapidly advancing field of Internet of technology (IoT) has extraordinary potential but carries with it many issues that may deleteriously affect user privacy, safety, and especially security (Atzori et al., 2010). Researchers have discovered that users frequently minimize this concern for security in favor of convenience and ease of use of the technology and that they expect ownership and security of their smart devices and data. (Bandyopadhyay and Sen, 2011).

Do perceived usefulness, effort expectancy, social influence, and facilitating conditions of the Smartwatch predict a consumer’s adoption of the smartwatch? The dependent variable is a consumer’s use of a Smartwatch (as measured by level of usage questions from the UTAUT). (See Appendix A – “Smart Technology” and IoT Use Survey). The independent variables are consumers’ perceived usefulness, effort expectancy, social influence, and facilitating conditions of the Smartphone and gender, age, experience with technology, and voluntariness of use (as measured by the UTAUT (See Appendix A – “Smart Technology” and IoT Use Survey).

The statistical procedure used to answer the question will be a multiple linear regression. As the primary statistic for analysis of a regression is the effect coefficient B (i.e., slope), the statistical hypotheses are:

Ha1: BPE ≠ 0, where BPE is the effect coefficient of a user’s perception of usefulness of the Smartwatch, that is, the perception of usefulness of the Smartwatch is a statistically significant predictor of a person’s use of or intent to use the Smartwatch.

Ha2: BEE ≠ 0, where BEE is the effect coefficient of a user’s perception of the expectancy of effort to use the Smartwatch, that is, the perception of expectancy of effort to use a Smartwatch is a statistically significant predictor of a person’s use of or intent to use the Smartwatch.

Ha3: BSI ≠ 0, where BSI is the effect coefficient of a user’s perception of the social influence in using a Smartwatch, that is, the perception of social influence is a statistically significant predictor of a person’s use of or intent to use the Smartwatch.

Ha4: BFC ≠ 0, where BFC is the effect coefficient of a user’s perception of conditions facilitating the use of a Smartwatch, that is, the perception of facilitating conditions is a statistically significant predictor of a person’s use of or intent to use the Smartwatch.

Ha5: Bgender ≠ 0, where Bgender is the effect coefficient of a user’s gender, that is, gender is a statistically significant predictor of a person’s use of or intent to use the Smartwatch.

Ha6: Bage ≠ 0, where Bage is the effect coefficient of a user’s age, that is, age is a statistically significant predictor of a person’s use of or intent to use the Smartwatch

Ha7: Bexperience ≠ 0, where Bexperience is the effect coefficient of a user’s with IoT and smart technology in general, that is, experience with techonology is a statistically significant predictor of a person’s use of or intent to use the Smartwatch

Ha8: Bvoluntariness ≠ 0, where Bvoluntariness is the effect coefficient of a user’s volunatirness of use, that is, voluntariness of use is a statistically significant predictor of a person’s use of or intent to use the Smartwatch

### Research Methodology

The research question will be answered using a multiple linear regression to test the statistical hypotheses. Data will be collected using a survey hosted online. The survey (see Appendix B – Smart Technology IoT Use Survey) will collect data to measure the dependent variable (adoption of Internet of Things/Smart technology), the primary independent variables (security, ease of use, and cost), and respondent demographics.

### Research Design

This will be a quantitative, correlational, non-experimental study using a multiple, linear regression procedure to determine if perceived usefulness, effort expectancy, social influence, and facilitating conditions of using the Smartwatch predict a consumer’s adoption of the smartwatch. The dependent variable is actual use of or intent to use a Smartwatch. Primary independent variables are UTAUT scores of perceived usefulness, effort expectancy, social influence, and facilitating conditions. Secondary independent variables are gender, age, experience with technology, and voluntariness of use of technology. Tertiary independent variables are education level, income, ethnic identity, and familiarity with smart technology. Data collection will be through completion of the online Smart Technology (IoT) Use Survey online hosted by SurveyMonkey™.

**Sample Selection**

The population under study will not be restricted or limited except that they must be at least 18 years of age so as not require permission from a guardian to participate. Participants will be selected from a convenience sample as it saves time and reduces expense. The disadvantage is that it is a non-probability sample and as such is usually regarded as difficult to generalize results. However, the population under study will be, intentionally, very broad with a wide range of experience with technology and would thus be more general in nature anyway.

An a-prior power analysis was performed to determine minimum sample size for a multiple regression of medium effect size (.15), alpha = .05 significance level, with statistical power of .80. As the maximum number of predictors could be as much as 9 in any one regression run (three IVs (Ha1, 2, and 3) + six demographics = 9 predictors), the computed sample size required for 9 predictors with a medium effect size of 0.15 (as per Cohen 1992) tested at the alpha = .05 level is 113.

**[Instrumentation](#_Toc351528707)**

An online survey through SurveyMonkey™ will be used for data collection (see Appendix B – Smart Technology/IoT Use Survey). The survey items were developed by the researcher for this study based on modifying the prior validated form of the UTAUT. According to the UTAUT model developers, the intent of the UTAUT was to modify for use with a specific technology (Vankatesh, et al, 2011).

The survey will collect data on the variables as follows –

* Questions 1–4, 10 and11 are designed to collect data on the extent of understanding the respondent has with the terms of Smart Tech and IoT and what they do;
* Questions 5-9 are demographics describing the respondent;
* Question 12 is designed to collect data on the level of experience the respondent has with smart technology;
* Question 13 and 14 are designed to collect data on how much smart technology is actually used;
* Questions 15 and 16 are designed to collect data on voluntariness of use of smart technology in general;
* Question 17 – 19 are designed to collect data on actual use of a Smartwatch;
* Questions 20-31 are the UTAUT survey (after Vankatesh, et al, 2011):
  + Perceived Usefulness (PE) -- Q20, 21, 22
  + Effort Expectancy (EE) – Q23, 24, 25
  + Social Influence (SI) – Q26, 27, 28
  + Facilitating Conditions (FC) – Q29, 30 31.

Questions and statements will be measured on a six-point Likert scale in several forms (see Appendix B – Smart Technology/IoT Use Survey) – strength of agreement (e.g., “strongly agree” to “strongly disagree”) and level of importance (e.g., “very good” to “very bad”). Only the extreme points are labeled as “intermediate labels tend to bias responses by suggesting a meaning to the value” (Hamby, 2019b, p. 56). The six-point scale is used to reduce central tendency bias, that is, the tendency for respondents not to take a position by selecting the center value in an odd-numbered scale. Grover, R. and Vreins, M., (2006) state “there is more midpoint [central tendency] responding when a middle category is expressly ordered.” (p. 105).

As the primary purpose of quantitative measurement is to measure the variation in a “variable”, measurement of every variable must strive to be measured at the highest level possible (given the nature of the variable) of the four levels of measurement – nominal, ordinal, interval/scale, and ratio. The demographic variable “age”, often exiguously measured as ordinal level (i.e., categories of age), will be measured at the ratio level, that is, the respondent will be asked simply to identify his/her age as respondents generally all know their ages and are usually not reluctant to reveal it (Hamby, 2019b). Income will be measured at the ordinal level only because respondents tend to be confused as to what type of income is asked for (e.g., after taxes, family, total, etc.) and don’t really know their income to within a thousand dollars. Deferring to social trends, gender will have a third category “other” to allow for those respondents who are sensitive to the issue (Hamby, 2019a). Ethnic identity is always difficult to define and evolves with society. For this study, the ethnic categories used will be those identified by the U.S. Department of Education and many other state and national agencies. Education level, likewise, will be measured at the ordinal level in that each category assumes a higher level of education.

### Validity and Reliability

Cronbach’s alpha measures internal consistency, i.e., how well a test measures what it was intended to measure. Cronbach’s alpha is particularly suitable to multiple-item Likert scale surveys (Tavakol, M. and Dennick, R., 2011). The rule of thumb for a robust measure of reliability is a Cronbach’s Alpha greater than .70. Several studies that used versions of the UTAUT modified for their specific context returned Cronbach’s Alpha greater than .70 (refer to studies by Madigan, et al. (2016), Bervell and Umar (2017), Abu-Dalbouh (2013), Vankatesh, et al. (2011), Alshehri, et al., 2011), Sarfaraz (2017), and Attuquayefio and Addo (2014)).

### Data Collection Procedures

SurveyMonkey™ will be commissioned to collect the sample as well as host the survey. SurveyMonkey™ uses diverse sites to actively seek participants based on the customer’s requirements to help ensure robust sampling. Its contact techniques include e-mail invitations, SMS and text messages, telephone alerts, banners and messaging on web sites and online communities. Recruited participants will be given a web-link to the survey posted on SurveyMonkey™. Individual responses from the completed survey will be downloaded in the form of an Excel™ file to be organized and entered into SPSS™ for statistical analysis. The primary analytical procedure will be a step-wise multiple regression procedure.

### Data Analysis Procedures

This study will use a multiple linear regression to test if the aforementioned independent variables are statistically significant predictors use of or intent to use a Smartwatch. The primary procedure used in all of the studies using UTAUT to explore people’s adoption of technology reviewed for this study have used a confirmatory factor analysis (CFA) or structural equations modeling (SEM) statistical procedure. However, these procedures are designed more to test the goodness of fit of a theorized model of the influence specified factors on a specified dependent variable than to actually predict the outcome of the influence. They are particularly good for determining causality, that is, if an independent variable actually “causes” an effect on a dependent variable. This study does not intent to determine if the UTAUT factors “cause” a respondent to adopt a Smartwatch but only want to predict if a person would probably a Smartwatch based on knowing the person’s responses to the factors. Therefore the best statistical procedure for the scope and purposes of this study is a multiple linear regression.

Each of the UTAUT factors become independent variables and, therefore, unique statistical hypotheses. Each hypothesis will be tested using a multiple, linear regression, stepwise procedure, to determine the correlation (multiple R), coefficient of determination (R-square), and actual predictive effects (B or “slope”) of the independent variables (perceived usefulness, effort expectancy, facilitating conditions, social influence, gender, age, experience with technology, voluntariness of use) on the dependent variable (consumer’s adoption of the Smatwatch). Statistical significance (confidence level) will be tested at the alpha = .05. The stepwise regression adds each variable sequentially as they are listed and removes it if it is found to be not statistically significant (usually at the alpha = .05 level, or as directed by the analyst).

Descriptive statistics (gender, age, education level, ethnic identity, income level and familiarity with smart technology) will be run and presented to describe the population. A Cronbach alpha test of reliability of the survey will be run to test validity and reliability of the survey. All statistics will be tested at the .05 significance level. All data will be analyzed on SPSS.

### Ethical Considerations and Procedures

Due care will be given to protect the privacy of the participants. IP address and geographical location identifier will be disabled. There will be no personally identifying data collected. The participant will click on a link that will automatically direct them to the survey questionnaire located on SurveyMonkey. The participants IP address will not be recorded or registered, thereby protecting the confidentiality and anonymity of the participant. The findings will be reported in the aggregate or totals instead of the results of individual responses.

### Summary of Research

This study is a quantitative, correlational, non-experimental design using a multiple linear regression on SPSS to determine if UTAUT factors perceived usefulness, effort expectancy, social influence, and facilitating conditions of the Smartwatch predict a consumer’s adoption of the smartwatch. The dependent variable is a consumer’s use of a Smartwatch (as measured by level of usage questions from the UTAUT. The independent variables are consumers’ perceived usefulness, effort expectancy, social influence, and facilitating conditions of the Smartphone and gender, age, experience with technology, and voluntariness of use (as measured by the UTAUT. Data will be collected using an online survey developed from the UTAUT with additional measures of actual use of or intent to use the Smartwatch. A post-hoc test of reliability of the survey will run and analyzed. Data will be collected from a convenience sample and the target population not restricted however all respondents must be at least 18 years of age so as not require permission from a guardian to participate.

REFERENCES

Ablon, L., & Libicki, M. (2015). Hackers’ bazaar: The markets for cybercrime tools and stolen data. Defense Counsel Journal, 82(2), 143–152.

Abu-Al-Aish, A., & Love, S. (2013). Factors influencing students’ acceptance of learning: An investigation in higher education. *International Review of Research in Open and Distance Learning,* 14(5).

Abu-Dalbouh, H. (2013). A questionnaire approach based on the technology acceptance model for mobile tracking on patient progress applications. *Journal of Computer Science* 9 (6): 763-770. Published Online 9 (6) 2013 (http://www.thescipub.com/jcs.toc)

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., & Lentz, M. (2015). Brave new world: Privacy risks for mobile users. ACM SIGMOBILE Mobile Computing and Communications Review, 18(3), 49–54. https://doi.org/10.1145/2721896.2721907

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for Internet of Things: A survey. Journal of Network and Computer Applications, 66, 198–213. https://doi.org/10.1016/j.jnca.2016.03.006

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, Volume 50, Issue 2, December 1991, Pages 179-211.

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. *Quality Progress,* 40(7), 64–65.

Alperovitch, D. (2014). The art of attribution: Identifying and pursuing your cyber adversary. Presented at the RSA Conference, San Francisco. Retrieved from http://www.rsaconference.com/writable/presentations/file\_upload/anf-t07b-theart-of-attribution-identifying-and-pursuing-your-cyber-adversaries\_final.pdf

Alshehri, M., Drew, S., Alhussain, T., & Alghamdi (2011). The effects of website quality on adoption of E-government service: an empirical study applying UTAUT nodel using SEM. 23rd Australasian Conference On Information Systems, Website Quality and E-Government Service, 3-5 Dec 2012,

Arce, I., Clark-Fisher, K., Daswani, N., DelGrosso, J., Dhillon, D., Kern, C., … Schoenfield, B. (2014). Avoiding the top 10 software security design flaws. IEEE Computer Society Center for Secure Design.

Asensio, A., Marco, A., Blasco, R., & Casas, R. (2014). Protocol and architecture to bring things into Internet of Things, protocol and architecture to bring things into Internet of things. International Journal of Distributed Sensor Networks, International Journal of Distributed Sensor Networks, 2014, 2014, e158252. https://doi.org/10.1155/2014/158252, 10.1155/2014/158252

Attuquayefio, S. N., & Addo, H. (2014). Using the UTAUT model to analyze students’ ICT adoption. International Journal of Education and Development Using Information and Communication Technology, 10(3), 75–86.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5

Bervell, B. and Umar, I. (2017). *validation of the UTAUT model: re-considering non-linear relationships of exogeneous variables in higher education technology acceptance research.* EURASIA Journal of Mathematics Science and Technology Education

Bojanova, I., Hurlburt, G., & Voas, J. (2014). Imagineering an Internet of anything. Computer, 47(6), 72–77. https://doi.org/10.1109/MC.2014.150

Bourke, B. (2014). Positionality: Reflecting on the research process. *The Qualitative Report,* *19*, 1-9. Available at: http://www.nova.edu/ssss/QR/QR19/bourke18.pdf

Calder, A., & Watkins, S. (2012). IT governance: An international guide to data security and ISO27001/ISO27002. Philadelphia: Kogan Page.

Capella University (2019). *Your literature review plan*. Retrieved from http://www.capella.edu/interactivemedia/library/litReviewTutorial/downloads/LitReviewPlan\_FinalCopy.pdf

Cebula, J., & Young, L. (2010, December). A taxonomy of operational cyber security risks. Pittsburgh, PA: Carnegie-Mellon Software Engineering Institute (SEI).

Chen, P.-Y., Cheng, S.-M., & Chen, K.-C. (2014). Information fusion to defend intentional attack in Internet of Things. IEEE Internet of Things Journal, 1(4), 337–348. https://doi.org/10.1109/JIOT.2014.2337018

Chen, Y., Ramamurthy, K. (Ram, & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. The Journal of Computer Information Systems, 55(3), 11–19.

Chen, Z., Xia, F., Huang, T., Bu, F., & Wang, H. (2013). A localization method for the Internet of Things. Journal of Supercomputing, 63(3), 657–674. https://doi.org/10.1007/s11227-011-0693-2

Cohen, Jacob. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 319–340.

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

Davis, F.D., (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International J. Man-Machine Studies*, 38: 475-487. DOI: 10.1006/imms.1993.1022

Delic, K. (2015). The third wave: The Internet of Things. Ubiquity, 2015(October), 1–4. https://doi.org/10.1145/2822527

Dlodlo, N., Foko, T., Mvelase, P., & Mathaba, S. (2012). The state of affairs in Internet of Things research. Electronic Journal of Information Systems Evaluation, 15(3), 244–258.

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of Things. Info : The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 16(3), 21–1.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016a). A middleware for the Internet of Things. International Journal of Computer Networks & Communications, 8(2), 159–178. https://doi.org/10.5121/ijcnc.2016.8214

Fishbein, M. and Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. 1st Ed. Addison-Wesley, Reading, Mass. Pp: 578.

Gangwar, H., Date, H., & Raoot, A. D. (2014). Review on IT adoption: Insights from recent technologies. Journal of Enterprise Information Management, 27(4), 502–488.

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of Internet of Things technology. Asia Pacific Journal of Marketing and Logistics, 26(2), 211–231.

Goguen, J. A., & Meseguer, J. (1982). Security policies and security models. In IEEE Symposium on Security and privacy (Vol. 12). Oakland, CA.

Grand Canyon University (2019). The path to a successful doctoral experience. “*Differentiating between forms of literature.”* Retrieved from https://lc.gcumedia.com/res811/find-your-purpose-the-path-to-a-successful-doctoral-experience/v1.1/chapter-4-differentiating-between-forms-of-academic-literature.html

Grover, R. and Vriens, M. (2006). *The handbook of marketing research: uses, misuses, and future advances*. Sage Publications, Thousand Oaks, CA.

Hahn, A., & Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. IEEE Transactions on Smart Grid, 2(4), 835–843. https://doi.org/10.1109/TSG.2011.2163829

Hamby, M. (2019a). Writing Research: a handbook to writing research articles and dissertations. Kendall-Hunt Publishing, Inc., Dubuque, IA

Hamby, M. (2019b). General acceptance of technology survey. Unpublished instrument. Retrieved from https://www.milesflight.com

Harrop, W., & Matteson, A. (2014). Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. Journal of Business Continuity & Emergency Planning, 7(2), 149–162.

Hurlburt, G. F., Voas, J., & Miller, K. W. (2012). The Internet of Things: A reality check. IT Professional, 14(3), 56–59.

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Science, 38*(2), 185-195.

Jammes, F. (2016). Internet of Things in energy efficiency: The Internet of Things. Ubiquity, 2016(February), 2:1–2:8. https://doi.org/10.1145/2822887

Jayakumar, H., Lee, K., Lee, W., Raha, A., Kim, Y., & Raghunathan, V. (2014). Powering the Internet of Things. In Proceedings of the 2014 International Symposium on Low Power Electronics and Design (pp. 375–380). ACM. https://doi.org/10.1145/2627369.2631644

Kang-juan, L., & Liu-qing, X. (2012). Study on the smart city and its economic and social effect based on the Internet of Things. Lecture Notes in Information Technology, 25, 242.

Karimova, G. Z., & Shirkhanbeik, A. (2015). Society of things: An alternative vision of Internet of Things. Cogent Social Sciences, 1(1). https://doi.org/10.1080/23311886.2015.1115654

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE Communications Surveys Tutorials, 15(1), 446–471. https://doi.org/10.1109/SURV.2012.013012.00028

Lacuesta, R., Palacios-Navarro, G., Cetina, C., Peñalver, L., & Lloret, J. (2012). Internet of Things: Where to be is to trust. EURASIP Journal on Wireless Communications and Networking, 2012(1), 203. https://doi.org/10.1186/1687-1499-2012-203

Madigan, R., Louw, T., Dziennus, M., Graindorge, T., Ortega, E., Graindorge, M., Merat, N. (2016). Acceptance of Automated Road Transport Systems (ARTS): an adaptation of the UTAUT model. 6th Transport Research Arena April 18-21, 2016, Transportation Research Procedia 14 (2016 ) 2217 – 2226).

Malik, A., Kumra, R., & Srivastava, V. (2013). Determinants of consumer acceptance of m-commerce. South Asian Journal of Management, 20(2), 102–126.

Mansfield-Devine, S. (2016). Securing the Internet of Things. Computer Fraud & Security, 2016(4), 15–20. https://doi.org/10.1016/S1361-3723(16)30038-0

Marias, G. F., Barros, J., Fiedler, M., Fischer, A., Hauff, H., Herkenhoener, R., …Vinhoza, T. T. V. (2012). Security and privacy issues for the network of the future: Security and privacy issues for the network of the future. Security and Communication Networks, 5(9), 987–1005. https://doi.org/10.1002/sec.384

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (3rd ed). Thousand Oaks, CA: Sage.

McLewndon, M. (1994). Multiple regression and causal analysis. FE Peacock, Inc. Itasca, IL

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. Journal of Information Privacy & Security, 10(4), 160–185.

Mishler, E. (1990). Validation in inquiry-guided research: The role of exemplars in narrative

Nakhuva, B., & Champaneria, T. (2015). Study of various Internet of Things platforms. International Journal of Computer Science & Engineering Survey, 6(6), 61–74. https://doi.org/10.5121/ijcses.2015.6605

Nayyar, A., & Puri, V. (2016). Data glove: Internet of Things (IoT) based smart wearable gadget. British Journal of Mathematics & Computer Science, 15(5), 1–12. https://doi.org/10.9734/BJMCS/2016/24854

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. Computer, 46(4), 46–53. https://doi.org/10.1109/MC.2013.74

Rogers, E. (1995). Diffusion of Innovations. 4th Ed. Free Press, New York, ISBN-10: 0028740742.

Sarfaraz, J. (2017). *Unified theory of acceptance and use of technology (UTAUT) model-mobile banking.* Journal of Internet Banking and Commerce. Journal of Internet Banking and Commerce, December 2017, vol. 22, no. 3.

Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6), 91–98. https://doi.org/10.1109/MWC.2013.6704479 studies. *Harvard Educational Review, 60,* 415-442.

Swan, M. (2012). Sensor mania! The Internet of Things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor and Actuator Networks, 1(3), 217–253. https://doi.org/10.3390/jsan1030217

Tao, F., Zuo, Y., Xu, L. D., & Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Transactions on Industrial Informatics, 10(2), 1547–1557. https://doi.org/10.1109/TII.2014.2306397

Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach’s Alpha. International Journal of Medical Education. 2011; 2:53-55 Editorial Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/

Thomas, T., Singh, L., & Gaffar K. (2013). *The utility of the UTAUT model in explaining mobile learning adoption in higher education in Guyana.* International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2013, Vol. 9, Issue 3, pp. 71-85

U.S. Census Bureau. (2018, July). Population estimates, July 1, 2018, (V2018). Retrieved July 1, 2018, from http://www.census.gov/quickfacts/

Varaiya, P. (1993). Smart cars on smart roads: problems of control. Automatic Control, IEEE Transactions on, 38(2), 195–207.

Venkatesh, A. (2008). Digital home technologies and transformation of households. Information Systems Frontiers, 10(4), 391–395. https://doi.org/http://dx.doi.org/10.1007/s10796-008-9097-0

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. 2003. User acceptance of information technology: toward a unified view, MIS Quarterly (27:3), pp 425-478.

Venkatesh, V. Thong, J.,Chan, F. Hu, P., & Brown, S. (2011). Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context. Information Systems Journal 21, p. 527–555 doi:10.1111/j.1365-2575.2011.00373.x

Venkatesh, V., L. 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.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3).

Venkatesh, V., Thong, J., & Xin Xu (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. Journal of the Association for Information Systems, vol.17, issue15.

Wakunuma, K. J., & Stahl, B. C. (2014). Tomorrow’s ethics and today’s response: An investigation into the ways information systems professionals perceive and address emerging ethical issues. Information Systems Frontiers, 16(3), 383–397. https://doi.org/http://dx.doi.org/10.1007/s10796-014-9490-9

Wang, C., Bi, Z., & Xu, L. D. (2014). IoT and cloud computing in automation of assembly modeling systems. IEEE Transactions on Industrial Informatics, 10(2), 1426–1434. https://doi.org/10.1109/TII.2014.2300346

Whitehouse, O. (2014, April 9). Security of things an implementers guide to cyber security for Internet of Things devices and beyond. London, UK: NCC Group.

Workman, M., Bommer, W. H., & Straub, D. (2008a). Information security questionnaire. PsycTESTS. https://doi.org/10.1037/t13417-000

Young, R. (2010). Evaluating the perceived impact of collaborative exchange and formalization on information security. Journal of International Technology and Information Management, 19(3), 19–37.

Zaslavsky, A., & Jayaraman, P. P. (2015). Discovery in the Internet of Things: The Internet of Things. Ubiquity, 2015(October), 2:1–2:10. https://doi.org/10.1145/2822529

APPENDIX A

**“Smart Technology” and IoT Use Survey**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **“Smart Technology” and IoT Use Survey**  *“Smart Technology” and Internet of Things (IoT) are essentially synonymous. The Internet of Things is about connecting devices and objects over the Internet allowing them to talk to each other and to us.* | | | | | |
| 1. Had you heard of IoT before this survey? YES NO | | 2. Had you heard of “Smart Technology” before this survey?  YES NO | | | |
| 3. How familiar are you with IoT (Internet of Things)? | Very Familiar Not at all  6 5 4 3 2 1 | | | | |
| 4. Off the top-of-your head, please write in as many examples of Smart Tech you can think of (Do not worry about spelling or punctuation) | | | | | |
| 5. What is your gender? *(circle one)* MALE FEMALE OTHER | | | 6. What is your age? \_\_\_\_\_\_\_\_\_\_\_\_. | | |
| 7. What is the highest level of education you have completed? *(circle one)*  HIGH-SCHOOL SOME COLLEGE UNDERGRADUATE GRADUATE DOCTORATE | | | | | |
| 8. What is your household income? *(circle one)*  <$20K $20 to $40K $40K to $60K $60K to $80K $80K to $100K >$100K | | | | | |
| 9. What is your ethnic identity? *(circle one)*  WHITE HISPANIC/LATINO BLACK/AFRICAN-AMERICAN NATIVE AMERICAN  ASIAN/PACIFIC ISLANDER OTHER *(PLEASE SPECIFY)* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| *Without necessarily thinking of any specific Smart Technology, please indicate your response to the following:* | | | | | |
| 10. How much do you use “Smart Technology” (Internet of Things (IoT) that you are aware of? | | | | Frequently Hardly ever  6 5 4 3 2 1 | |
| 11. How familiar are you with where and how smart technology is being used? | | | | Very familiar Not at all  6 5 4 3 2 1 | |
| 12. How much experience have you had with smart technology? | | | | A Lot Hardly any  6 5 4 3 2 1 | |
| 13. How frequently do you intentionally interact with smart technology? | | | | Very Often Hardly ever  6 5 4 3 2 1 | |
| 14. How frequently do you think you are interacting with smart technology? | | | | Very Often Hardly ever  6 5 4 3 2 1 | |
| 15. How readily do you adopt a new technology in your daily activities? | | | | Quite readily I resist it!  6 5 4 3 2 1 | |
| 16. What is your general attitude towards the utility of smart technologies? | | | | Can’t live I really  without it don’t want it  6 5 4 3 2 1 | |
| 17. Regards a **Smartwatch** specifically, how often do you use it for other than just telling the time? | | | | Frequently Hardly ever  6 5 4 3 2 1 | |
| 18. If you *have* a **Smartwatch**, do you intend to continue to use it? | | | Definitely Probably not  6 5 4 3 2 1 | | Don’t have one |
| 19. If you do *not* have a **Smartwatch**, do you intend to get one? | | | Definitely Probably not  6 5 4 3 2 1 | | Already have one |
| *Please indicate your strength of agreement with the following statements.* | | | | | |
| 20. Using a Smartwatch enables or would enable me to put more into my daily activities. | | | | Strongly Agree Strongly Disagree  6 5 4 3 2 1 | |
| 21. Using a Smartwatch makes or would make it easier to live my daily activities. | | | | 6 5 4 3 2 1 | |
| 22. Using a Smartwatch enhances or would enhance my effectiveness of my daily activities. | | | | 6 5 4 3 2 1 | |
| 23. I find or would find it easy to use a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |
| 24. Learning to use a Smartwatch for my daily activities is or would be easy for me. | | | | 6 5 4 3 2 1 | |
| 25. It is or would be easy for me to become skillful at adapting a Smartwatch to my daily activities. | | | | 6 5 4 3 2 1 | |
| 26. People who influence my behavior think or would think that I should use a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |
| 27. People who are important to me think or would think that I should use a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |
| 28. People who are in my social circle think or would think that I should use a Smartwatch to in my daily activities. | | | | 6 5 4 3 2 1 | |
| 29. I have the resources necessary to use a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |
| 30. I have the knowledge necessary to use a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |
| 31. Technical support is or would be available for assistance with difficulties using a Smartwatch in my daily activities. | | | | 6 5 4 3 2 1 | |

EXAPLANATION

The following description of the questions does not appear on the survey and is not presented to the respondent.

Questions 1–4, 10 and11 are designed to collect data on the extent of understanding the respondent has with the terms of Smart Tech and IoT and what they do.

Questions 5-9 are demographics describing the respondent.

Question 12 is designed to collect data on the level of experience the respondent has with smart technology

Question 13 and 14 are designed to collect data on how much smart technology is actually used

Questions 15 and 16 are designed to collect data on voluntariness of use of smart technology in general

Question 17 – 19 are designed to collect data on actual use of a Smartwatch.

Questions 20-31 are the UTAUT survey (after Vankatesh, et al, 2011).

* Perceived Usefulness (PE) -- Q20, 21, 22
* Effort Expectancy (EE) – Q23, 24, 25
* Social Influence (SI) – Q26, 27, 28
* Facilitating Conditions (FC) – Q29, 30 31

APPENDIX B

Permission to Use UTAUT Instrument

Following is an email from the author of the UTAUT granting perimsioon to use the UTAUT for this study:

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**From:** site@vvenkatesh.com <site@vvenkatesh.com>  
**Sent:** Tuesday, November 5, 2019 8:41 AM  
**To:** Ala Abutabanjeh <ala.ali1@outlook.com>  
**Subject:** Papers-Permissions/Download

Thank you for your interest. Your permission to use content from the paper is granted. Please cite the work appropriately. Note that this permission does not exempt you from seeking the necessary permission from the copyright owner (typically, the publisher of the journal) for any reproduction of any materials contained in this paper.

Sincerely,  
Viswanath Venkatesh  
Distinguished Professor and George and Boyce Billingsley Chair in Information Systems  
Email: vvenkatesh@vvenkatesh.us  
Website: http://vvenkatesh.com