TECHNOLOGY ACCEPTANCE MODEL TO EVALUATE FACTORS AFFECTING ADOPTION OF THE INDUSTRIAL INTERNET OF THINGS (IIOT) BY THE INDUSTRIAL PROFESSIONALS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS OF
THE MIDDLE EAST TECHNICAL UNIVERSITY
BY

SERTAN SELÇUK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF CYBERSECURITY

NOVEMBER 2021

Approval of the thesis:

TECHNOLOGY ACCEPTANCE MODEL TO EVALUATE FACTORS AFFECTING ADOPTION OF THE INDUSTRIAL INTERNET OF THINGS (IIOT) BY THE INDUSTRIAL PROFESSIONALS

Submitted by Sertan Selçuk in partial fulfillment of the requirements for the degree of **Master of Science in Cyber Security Department, Middle East Technical University** by,

Prof. Dr. Deniz Zeyrek BOZŞAHİN
Dean, **Graduate School of Informatics** ______________________

Asst. Prof. Dr. Cihangir TEZCAN
Head of Department, Cyber Security, METU ______________________

Assoc. Prof. Dr. Cengiz ACARTÜRK
Supervisor, Cognitive Science Dept., METU ______________________

Examining Committee Members:

Asst. Prof. Dr. Cihangir TEZCAN
Cyber Security Dept., METU ______________________

Assoc. Prof. Dr. Cengiz ACARTÜRK
Cognitive Science Dept., METU ______________________

Asst. Prof. Dr. Murat ULUBAY
Management Dept., Ankara Yildirim
Beyazit University ______________________

Date: 24 November 2021

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Sertan Selçuk

Signature :

ABSTRACT

TECHNOLOGY ACCEPTANCE MODEL TO EVALUATE FACTORS AFFECTING ADOPTION OF THE INDUSTRIAL INTERNET OF THINGS (IIOT) BY THE INDUSTRIAL PROFESSIONALS

Selçuk, Sertan

MSc., Department of Cyber Security

Supervisor: Assoc. Prof. Dr. Cengiz Acartürk

November 2021, 164 pages

The use of the Industrial Internet of Things (IIoT) is increasing rapidly. In this way, with the ability to collect and analyze vast amounts of data, operational costs began to decrease, product quality improved, and human errors started to decline dramatically.

However, with the opening of production facilities to the Internet, many organizations have become direct targets of attackers. Security infrastructures of organizations, reliability of systems, the safety of facilities, and confidentiality of information have gained more importance than ever before. On the other hand, the interoperability of new IIOT enabled systems and their integration into existing systems turned out to be challenging due to lack of standards, heterogeneity, and insufficiently qualified resources.

This study aims to identify the factors affecting the adoption of IoT technology by industries. The research includes qualitative research conducted with 11 industry experts and quantitative data analysis collected from 342 industry experts from different regions worldwide. The quantitative research results were analyzed with a conceptual model developed based on the Technology Acceptance Model using Structural Equation Modelling with Partial Least Squares (SEM-PLS).

As the output of the study, two factors, perceived risk, and perceived trust, came to the fore with high effect values. The study provides the basis for solution providers, end-users, policymakers, and researchers to take measures to reduce security risks and make systems work better together.

Keywords: Industrial Internet of Things (IIoT), IIoT Adoption, Industry 4.0, Smart-connected systems, Technology Acceptance Model

ÖZ

SEKTÖR UZMANLARI TARAFINDAN ENDÜSTRİYEL NESNELERİN İNTERNETİ'NİN (IIOT) BENİMSENMESİNİ ETKİLEYEN FAKTÖRLERİ DEĞERLENDİRMEK İÇİN TEKNOLOJİ KABUL MODELİ

Selçuk, Sertan
Yüksek Lisans, Siber Güvenlik Bölümü
Tez Yöneticisi: Doç. Dr. Cengiz Acartürk

Kasım 2021, 164 sayfa

Endüstriyel Nesnelerin İnterneti (IIoT) kullanımı hızla artıyor. Bu sayede büyük miktarda veri toplama ve analiz etme yeteneği ile operasyonel maliyetler düşmeye, ürün kalitesi iyileşmeye ve insan hataları önemli ölçüde azalmaya başladı.

Ancak üretim tesislerinin internete açılmasıyla birlikte birçok kuruluş doğrudan saldırganların hedefi haline geldi. Kuruluşların güvenlik altyapıları, sistemlerin güvenilirliği, tesislerin güvenliği ve bilgilerin gizliliği her zamankinden daha fazla önem kazanmıştır. Öte yandan, yeni IIOT özellikli sistemlerin birlikte çalışabilirliği ve bunların mevcut sistemlere entegrasyonu, standartların olmaması, heterojenlik ve yetersiz nitelikli kaynaklar nedeniyle zorlu hale geldi.

Bu çalışma, IoT teknolojisinin endüstriler tarafından benimsenmesini etkileyen faktörleri belirlemeyi amaçlamaktadır. Araştırma, 11 sektör uzmanıyla yürütülen nitel araştırmayı ve dünya çapında farklı bölgelerden 342 sektör uzmanından toplanan nicel veri analizini içermektedir. Nicel araştırma sonuçları, Kısmi En Küçük Karelerle Yapısal Eşitlik Modellemesi (SEM-PLS) kullanılarak Teknoloji Kabul Modeli temel alınarak geliştirilen kavramsal bir model ile analiz edilmiştir.

Çalışmanın çıktısı olarak iki faktör, algılanan risk ve algılanan güven, yüksek etki değerleri ile öne çıkmıştır. Çalışma, çözüm sağlayıcıların, son kullanıcıların, politika yapıcıların ve araştırmacıların güvenlik risklerini azaltmak ve sistemlerin birlikte daha iyi çalışmasını sağlamak için önlemler alması için temel sağlar.

Anahtar Kelimeler: Endüstriyel Nesnelerin İnterneti (IIoT), IIoT Benimseme, Endüstri 4.0, Akıllı bağlantılı sistemler, Teknoloji Kabul Modeli

To My Family

ACKNOWLEDGMENTS

First, I would like to thank my thesis advisor Associate Professor Dr. Cengiz Acartürk, who encouraged me to complete this thesis under difficult pandemic conditions and always supported me with his enlightening information and guiding advice.

I would like to extend my respects and thanks to all METU Informatics Institute lecturers who have enriched my cyber security knowledge and enabled me to apply the knowledge I gained at the institute in my professional life.

I want to thank my friends in the Department of Cyber Security at the METU Informatics Institute for their valuable contributions and ideas, each of whom I see as a gem and who accompanied me on my three-year METU journey. Additionally, I want to thank the industry experts who spared time during their busy work schedules, enlightened me with their opinions, and helped shape my thesis.

Finally, I would like to thank my beloved wife and children. They motivated me to go to Ankara every week for three years and encouraged me to receive a master's degree at a university like METU from the very beginning.

Sincerely,

Sertan Selçuk

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ANOVA	Analysis of Variance
AVE	Average Variance Extracted
CPS	Cyber Physical Systems
CR	Composite Reliability
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
ITU	International Telecommunications Union
KMO	Kaiser-Meyer-Olkin
OT	Operational Technology
PLS	Partial Least Squares
PoC	Proof of Concept
SCADA	Supervisory Control and Data Acquisition
TAM	Technology Acceptance Model
TOE	Technology, Organization, and Environment
UI	User Interface
UTAUT	Unified Theory of Acceptance & Use of Technology

CHAPTER 1

INTRODUCTION

The use of Industrial IoT (IIoT) technology, which is one of the critical components of the "Industry 4.0" revolution, has been spreading rapidly in recent years (Boyes et al., 2018). These smart connected devices have entered our lives with the manifesto of ubiquitous computing (Almomani et al., 2018), enabling industry professionals to control data streams anytime, anywhere. In this way, data collection and analysis, which were impossible in many sectors before or could be done with limited methods, can be performed automatically in real-time in huge volumes and short periods (Seetharaman et al., 2019; Nicolescu et al., 2018).

Today, an organization effectively using IIoT technology can eliminate human errors affecting production speed and product quality, automatically manage its supply chain, and eventually gain a significant competitive advantage. (Pizon, Klosowski & Lipski, 2019; Cao et al., 2019). IoT Analytics predicts that the number of interconnected IoT devices will more than triple by 2025 from 14 billion today (IoT Analytics report, 2020). The researchers also agree that with the development of other emerging technologies such as 5G, artificial intelligence, digital twin, blockchain, and 3D printing, users will soon adopt IIoT technology even more strongly. (Al-Turjman & Al-Turjman, 2018; Liu et al., 2019; Tange at al., 2019; Khalil et al., 2021; Khan & Salah, 2018).

In contrast, the coexistence of so many direct benefits has naturally caused organizations from various sectors to adopt IIoT technology in a shorter time than it might have been (Sengupta, Ruj, & Das Bit, 2020). The sudden opening of production lines and critical infrastructures to the outside world brought many problems to be carefully addressed. These issues can be listed as heterogeneity arising from the integrated operation of many systems, deficiencies of standards, trust problems related to cyber security, reliability, privacy, security, and safety, insufficient skilled human resources, and inadequacies of stakeholders (Moore et al., 2020; Hameed, Khan & Hameed, 2018; Saleem et al., 2018; Ahemd, Shah, & Walid, 2017).

Consequently, it becomes essential for technology providers, decision-makers, and researchers to identify the factors that positively or negatively affect the adoption of IIoT technology by industry professionals. However, studies measuring whether the benefits of IoT technology outweigh the existing problems due to the difficulties of accessing experts have remained very few and narrow.

This study aims to reveal the factors affecting the adoption of IIoT technology by professionals working in various regions and industries and evaluate the relationship between these factors. In this way, further enhancements can be performed within the IIoT ecosystem more effectively, ensuring that the systems seamlessly integrate and securely communicate with each other.

1.1. Problem Statement

According to Cisco's research conducted in 2016 with 1,845 organizations across the US, the UK, and India, more than 60% of IIoT projects fail the Proof of Concept (PoC) stage. Worse still, no more than a third of completed projects are considered successful (Cisco, 2017). The following reasons may be behind the termination of the projects at the PoC stage before they are implemented.

Kamal et al. point out the significance of security challenges arising from the convergence of IT and OT environments in their studies (Kamal et al., 2016). These types of attackers can cause significant disruptions, such as shutting down production lines, critical infrastructures and compromising millions of systems worldwide (Stellios et al., 2018; Panchal, Khadse & Mahalle, 2018).

Two different studies conducted by Madugula and Thiagarajan emphasize the importance of management support and the abilities of company employees and business partners to manage an IIoT project (Madugula, 2021; Thiagarajan, 2016). Besides, Sisinni et al. highlight the heterogeneity situation of the IIoT systems in their studies and pay attention to interoperability as a considerable barrier for the users to adopt the technology (Sisinni et al., 2018). Friedman and Goldstein point out another aspect of the heterogeneity problem and state that in a world where 14 billion are interconnected, a library of standards specific to IIoT technology has not yet been created (Friedman & Goldstein, 2019).

From a financial perspective, Accenture touches on the hidden costs of delivering IIoT services in their survey report and reveals that it's challenging to predict and stick to a specific budget plan on an IIoT project (World Economic Forum, 2015). Goundar et al. also join the discussion by highlighting other expenses such as recurring fees, maintenance costs, and consumables in the IIoT implementation projects (Goundar et al., 2021).

In light of the above statements, this study aims to review the literature on IIoT technology, identify the core values and challenges, and eventually propose a framework to evaluate users' perceptions towards adopting IIoT technology.

1.2. Research Objectives

The main objective of this research study is to effectively evaluate employees' adoption of IIoT technology with all its factors by developing a model that is as simple and understandable as possible.

In line with this primary goal, we will aim to measure the effectiveness of the factors we have mentioned below. In this context, we have shaped our study and developed our framework based on the Technology Acceptance Model considering the following objectives:

- To evaluate perceived usefulness and ease of use by the professionals and identify how these factors influence behavioral intentions of the users to adopt IIoT technology.
- To determine whether perceived risks arising from security concerns, safety issues, reliability problems are a barrier to adopting IIoT technology by industries.
- To identify whether users' motivations and future expectations may affect users' perceptions.
- To assess business partners and identify how users' trust in these third parties may affect the adoption of IIoT technology.
- To evaluate the cost-efficiency of the IIoT projects identifying in what degrees users perceive the benefits overweigh the costs and whether entry costs might be an obstacle to adopting the technology.
- To reveal the importance of management support in IIoT projects and evaluate how facilitating conditions may influence the users to adopt the technology.

1.3. Research Questions

Based on our targets, we have developed our research questions as follows:

1) What is the current state of technology acceptance of IIoTs in literature?
2) What are the main factors influencing users' behavioral intentions to adopt IIoT technology?
3) How are these factors affecting each other?

In line with our research questions, we also aim to reach findings that would provide answers to the following questions:

- Which technology models and how are they used to assess users' perceptions of accepting IIoT?
- What are their sample sizes? And which countries do they cover?
- *(Based on our qualitative research)* What are users' motivating factors, challenges, and expectations?
- *(Based on our qualitative research)* How do these users see the future of IIoT? What other emerging technologies are they planning to deploy?

1.4. Significance of the research

Despite challenges during the commissioning and operation of projects, IIoT is growing aggressively. Grandview Research Company forecasts the market size of Industrial IoT to be US$600 by 2025, up from US$216 billion in 2020 (Grandview Research Company, report, 2021). Mordor Intelligence, focusing on the consumer side, estimates the size of the consumer IoT market to reach US$985 by 2025, up from US$760 billion (Mordor Intelligence, report, 2021).

From these freshly published reports, we can conclude that the share of the IIoT market within the IoT cluster will more than double by 2025, indicating the increase of adoption of IIoT technology among industry professionals.

However, we have revealed from our preliminary literature review that most of the studies conducted on evaluating users' perceptions are explicit to consumer IoT technologies, including wearables, smart gadgets, and smart home devices. In contrast, the studies carried on the industrial IoT (IIoT) side have remained very narrow due to insufficient samples and covering only one country.

Our research study, with its targeted audience entirely from industries including manufacturing companies, energy providers, telco operators, ISPs, and retail companies, and its structure, which includes quantitative and qualitative research, can close this gap. Moreover, with the model presented at the end of this study, users' technology adoption can be easily measured and evaluated.

1.5. Thesis Structure

This study evaluates the key factors that play a role in adopting IIoT technology by manufacturing industries. In this case, we have identified the problem statements to adopting IIoT technology by industry users and asked our research questions. We then expressed our motivation and emphasized the significance of this research.

Chapter 2 will review the existing literature around IIoT technology and the Technology Acceptance Model that will form the basis of our model. Based on the discussions carried out in this section, the gaps will be identified, and further ideas will be given to improve IIoT technology adoption among industry professionals. Chapter 3 will present the hypotheses based on the literature research findings and develop a survey structure to evaluate these hypotheses. Chapter 4 will analyze the survey results and propose the model that fits users' perceptions of adopting the IIoT technology.

The final chapter will further discuss the results and propose solutions on a per-component basis to reduce the risks to technology adoption. In addition, this section will include the limitations encountered throughout the study and further research.

The structure that will be followed throughout the study is as given in Figure 1 below:

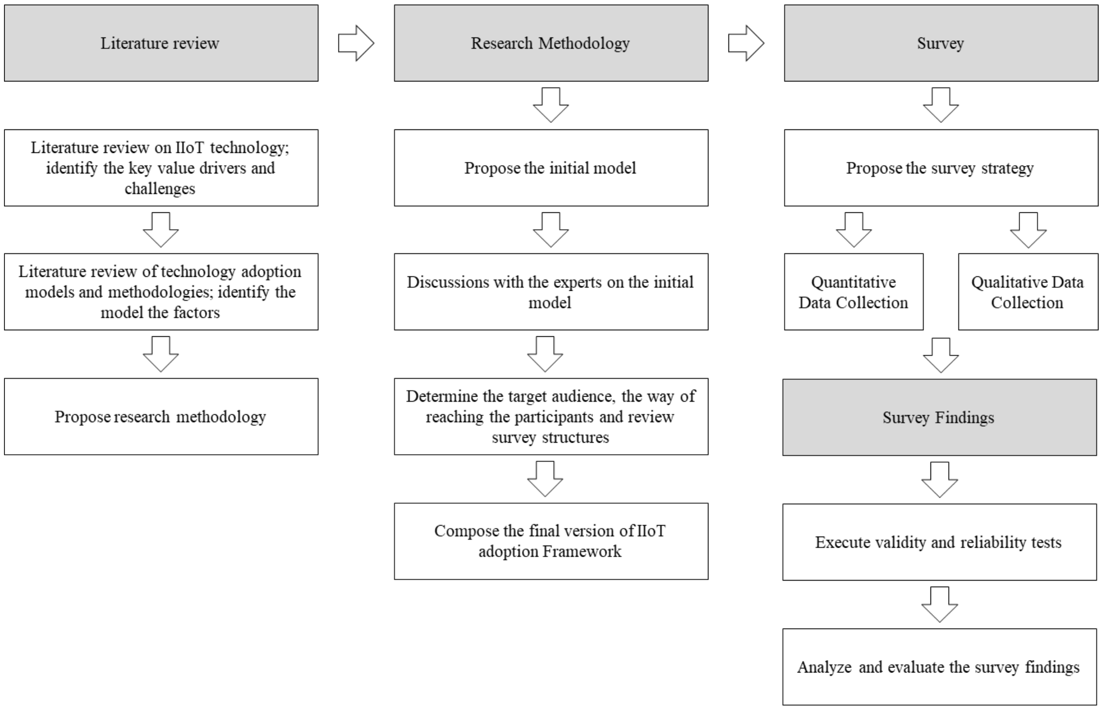


Figure 1 Thesis Structure

CHAPTER 2

LITERATURE REVIEW

This chapter contains an extensive review of literature carried out in three subcategories. The first part will examine the general definitions, components, and structures of IIoT technology. After that, the benefits and challenges of IIoT technology will be identified and discussed in detail. Chapter 2 will continue with a systematic review of technology adoption models and conclude with an explanation for choosing the Technology Acceptance Model for this study.

During the research, the following databases have been utilized: Google, Google Scholar, Scopus, IEEE Xplore, Elsevier, ScienceDirect, and METU Library.

2.1. Internet of Things (IoT)

Vongsingthong and Smanchat describe the IoT as a network of uniquely identified physical objects, things, and devices connected over the Internet (Vongsingthong & Smanchat, 2014). Likewise, Patel and Patel note that IoT Technology assigns each object a unique identification, making it possible to share data and central control mechanisms without human intervention (Patel & Patel, 2016). However, as Perwej et al. highlight, IoT is not a newly developed idea since the devices on the field have already been communicating with each other for many years. Kevin Ashton, the co-founder of the Auto-ID Center at MIT, firstly used the term "Internet of Things" in 1999 in his presentation made to Procter & Gamble (P&G) in 1999 (Perwej et al., 2019).

Berte touches on the usage areas of IoT technology and states that IoT devices are the technology tools such as smartphones and wearable devices, smart home devices like smart meters, security cameras, and industrial devices like intelligent machines. These smart connected devices can gather, share, and analyze information and create actions accordingly (Berte, 2018).

IIoT, on the other hand, is a new concept that has been developed later and addresses industrial applications (Zhou et al., 2017). The following parts of our research are entirely on IIoT.

2.2. Industrial Internet of Things (IIoT)

Neuroimaging Boyes et al. categorize the industrial Internet of things (IIoT) as a subset of the IoT while positioning IIoT as the deployment and use of IIoT devices in industrial sectors and applications (Boyes et al., 2018). According to TrendMicro, the IIoT technology enables industries and organizations to have better efficiency and reliability in their operations, focusing on machine-to-machine (M2M) communication, big data, and machine learning. In addition, the technology covers industrial applications, including robotics, medical devices, and software-defined production processes (TrendMicro Report, 2020).

Bedhief et al. state that since internet-enabled industrial networks are highly heterogeneous, industrial processes set new requirements such as reliability, scalability, and low latency that traditional technologies cannot manage (Bedhief et al., 2019). Moura et al. look at the enormous size of the data that is in motion in industrial places and mention that this massive amount of data requires the provision of information technology services with diversity and sufficient capacity to support the growing demand. They also claim in their study that creating this foundation infrastructure completely on-premises is often not feasible because it requires scalability and elasticity that would entail higher investments (Moura et al., 2018).

According to Sengupta and Dasbit, IIoT technology is built on SCADA technology due to its features in the following four areas (Sengupta, Ruj & Das Bit, 2020; Manditereza, 2017):

- **Scalability:** An IIoT system can build new facilities as needed using resources gathered from the cloud.
- **Data Analytics:** An IIoT system needs to allow for long-term data storage. Big data processing and machine learning techniques can be applied to predict results.
- **Standardization:** IIoT aims to standardize sensor networks, data collection, and aggregation to allow real-time communication within facilities.
- **Interoperability:** Through gateways, IIoT uses protocols such as Message Queuing Telemetry Transport (MQTT) that provide platforms that can be communicated and programmable between devices regardless of vendors.

2.2.1. The Differences Between IoT and IIoT

Both IoT and IIoT concepts have the same main characteristics of availability, intelligence, and connections capability. The only difference between those two is their general usages. While IoT is widely used for consumer usage, IIoT is used for industrial purposes such as monitoring the manufacturing processes, managing the supply chain, or controlling the management systems (CTI Group Report, 2016).

IoT is often described as a **revolution** (Sisinni et al., 2018) that will change life as we know it. However, IIoT is often described as an **evolution** (Sisinni et al., 2018) that will be applied more slowly across industries as different industrial markets evolve their specific needs and address their unique challenges (Schneider Report, 2015). IoT tends to be consumer-level devices with a low-risk impact when a failure occurs. They are essential and valuable, but malfunctions do not immediately create emergencies.

IIoT, on the other hand, connects critically important machines and sensors in high-stakes industries such as aerospace, defense, healthcare, and energy. These are the systems where failure often results in life-threatening or other emergencies (CTI Group Report, 2016).

It is undoubtedly accepted that IoT devices will grow higher with lower prices than IIoT, considering its production volume and technology capabilities. In contrast, IIoT is developed to process critical machines. Therefore, more sensitive sensors must be used in facilities, including sophisticated, advanced controls and analytics on the supply chain side (CTI Group Report, 2016). Based on these definitions, notable differences between IoT and IIoT can be listed in Table 1 below:

Table 1 Differences between IoT and IIoT (adapted from Sisinni et al., 2018)

	IoT Technology	Industrial IoT Technology
Impact	Revolution	Evolution
Audience	Consumers	Industries
Applications	General applications, including wearables, robots, and machines	Industrial applications
Criticality	No life-threatening	Uses critical equipment and devices connected over a network that may cause life-threatening or other emergency failures.
Scalability	Deals with small-scale networks.	Deals with large-scale networks.
Security	Requires identity and privacy	Requires robust security to protect the data
Requirements	Needs moderate requirements	Needs strict requirements
Lifecycle	Much shorter product lifecycle	Very long lifecycle
Reliability	Less reliability	High reliability
Connectivity	Ad hoc connectivity	Structured connectivity

2.2.2. Market Size & Opportunity

According to the Grandview Research Company report, published in 2021, the global IIoT market size was reported to be approximately US$216 billion in 2020 and is expected to exceed US$600 billion by 2025, growing with an average annual rate of 22.8%.

The same company also reports that aggressive IIoT adoption rate in line with technological advances and the easy availability of affordable sensors and processors that can facilitate real-time access to information are expected to drive IIoT market growth during the forecast period. The need to increase operational competence linked to solid collaboration among key market players to achieve the same is expected to drive market expansion. In addition, strategies to create a unified digital-human workforce are expected to create significant growth opportunities (Grandview Research Company, report, 2021). According to Allied Market Research Company's report published in 2018, the integration of intelligent devices into the industrial machines heartened the manufacturers to reduce the operational cost by 50% and is expected to decrease further (Allied Market Research Company, report, 2018).

According to one another report published by Mordor Intelligence in 2021, the global IoT market size was reported to be approximately US$761 billion in 2020 and is expected to exceed US$985 billion by 2025 with an average annual growth rate of 10.53% (Mordor Intelligence, report, 2021).

These two reports show that the share of the IIoT market within the IoT cluster will more than double by 2025, indicating the increase of adoption of IIoT technology among industry professionals. Market shares of both technologies are shown in Figure 2 below:

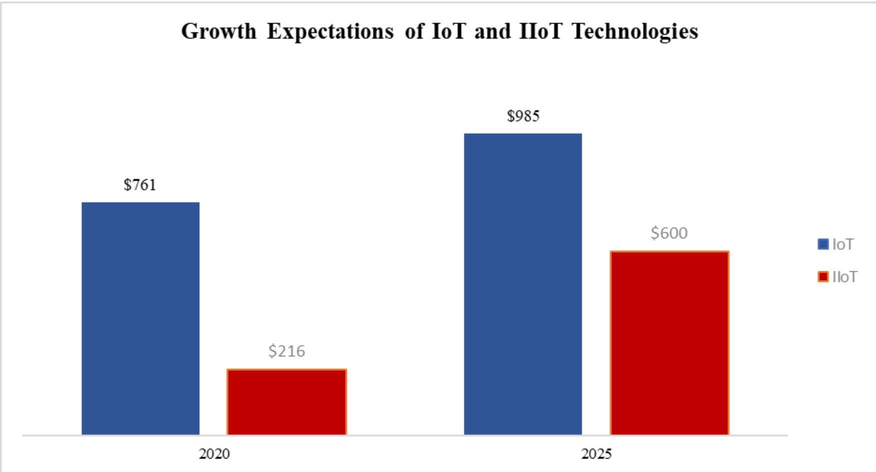


Figure 2 IoT and IIoT Market Shares by 2021 and 2025
Sources: Grandview Research Company Report, 2021; Mordor Intelligence Report, 2021, *(redrawn by the author)*

Considering the increase in the share of the Industrial IoT market in the next five years and the definitions in the previous two sections, it can be predicted that IIoT will accelerate its growth in the coming years and go beyond the scope of IoT.

2.2.3. IIoT Ecosystem

Bansal and Kumar define the IoT/IIoT ecosystem as a system that brings together all the heterogeneous components of IoT in a managed way to build an efficient system. It integrates devices, operating systems, controllers, gateways, middleware, and platform (Bansal & Kumar, 2020).

Rimmer from PWC summarizes the IIoT ecosystem and the functions of the components as in Figure 3 below:

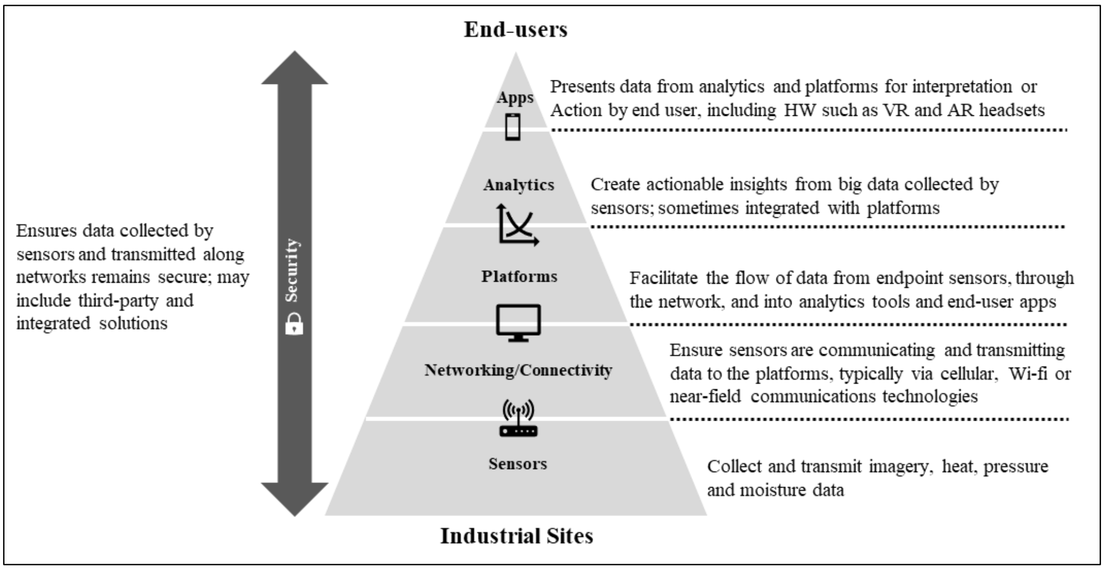


Figure 3 IIoT Ecosystem
Source: PWC Report, 2017 *(redrawn by the author)*

These elements are connected through communication protocol and interfaces, discussed in the next section.

2.2.4. IIoT in the Context of Industry 4.0

The first three industrial revolutions were driven by machinery, electrical energy, and automated production (Lukac, 2015; Haradhan, 2019). Hermann et al. describe Industry 4.0 as integrating the Internet into the value chain (Hermann et al., 2016). Lampropoulos et al. suggest that data collection, analysis, and comprehension from different sources, including production systems and equipment and customer management enterprise systems, will become the norm to support decision-making in real-time in the Industry 4.0 context (Lampropoulos et al., 2019).

Evans states that the fourth industrial revolution enables organizations to progress faster and more aggressively than three revolutions. He also lists the components of Industry 4.0, including big data, autonomous machines and robotics, artificial intelligence, nanotechnology, distributed ledger, and the Internet of Things (Evans, Cisco Report, 2011).

The four industrial revolutions can be summarized in Figure 4 below:

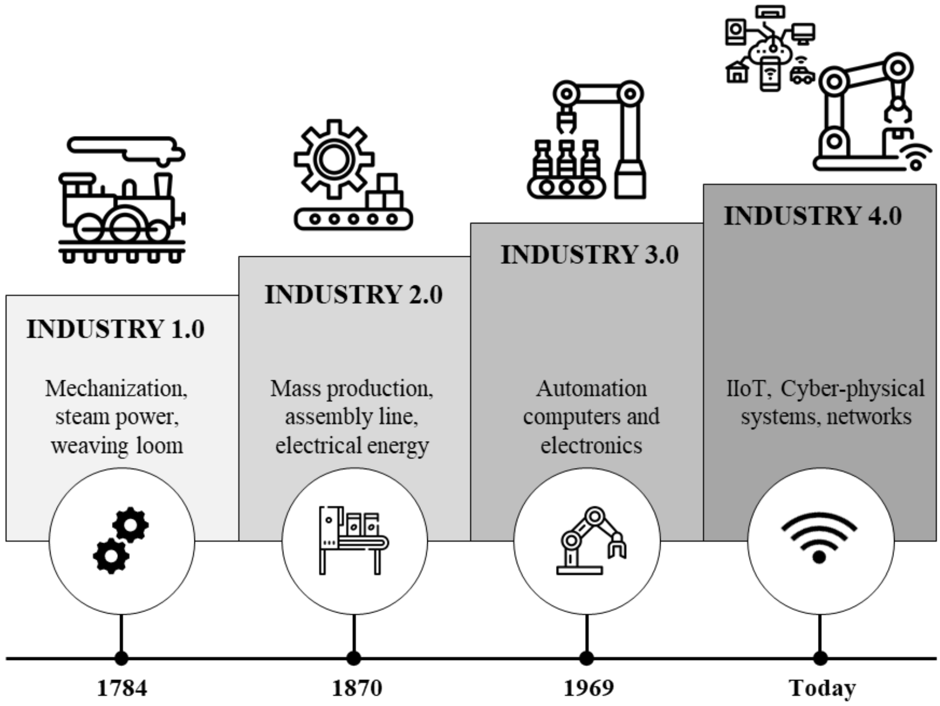


Figure 4 The Four Industry Revolutions
Source: Khalil et al., 2021 *(redrawn by the author)*

International Society of Automation (www.isa.org) emphasizes that the Internet of Things is the key enabling technology in Industry 4.0. Besides, Lampropoulos et al. also note that the Internet of Things (IoT) is a rapidly growing technology that significantly contributes to the realization of Industry 4.0 (Lampropoulos et al., 2019). Menezes, Kelly, and Leal have positioned IoT technology as one of the essential elements within the scope of Industry 4.0. According to their research, other elements of Industry 4.0 are autonomous robots, advanced analytics, system integration, cybersecurity, cloud computing, human-machine communication, advanced sensing, and big data (Menezes, Kelly & Leal, 2019).

Lampropoulos et al. conclude their studies about IoT in the context of Industry 4.0 that with the implementation of Industry 4.0 and IoT technologies, businesses can achieve unprecedented levels of economic growth and production efficiency such as:

- Development of production systems as more flexible and interoperable with other systems,
- Efficiency, speed, and quality improvement, particularly in engineering, operations, management, and decision making,
- Improvement in general applications, services, and procedures,
- Reduced lead times resulting in accelerated productivity and reduced time to market,
- Addressing individualized customer requirements and market demands,

- Improvements in monitoring and controlling enterprises' processes and assets,
- Reduced overall costs and waste,
- Decentralization and digitalization of production, *and*
- The capability of robust, enterprise-wide data analytics.

These discussions reveal the necessity of IIoT technology within the Industry 4.0 environment, pointing out the system's primary purpose as collecting and analyzing extensive data from the machines in the field and eventually performing the necessary optimizations to reduce costs and increase quality.

2.2.5. IIoT and Cyber-Physical Systems

Cyber-physical systems (CPS) are emerging technologies that deeply affect our society in various application areas. Some of these applications include autonomous aerial vehicles, wireless sensor networks, semi or fully autonomous cars, vehicular networks, and a new generation of sophisticated life-critical and networked medical devices (Ratasich et al., 2019). Singh et al. state that the interaction of physical components and the computational components is at the heart of Cyber-Physical Systems (Singh et al., 2019).

Ratasich et al. also point out that CPS consists of collaborative computational entities tightly interacting with physical components through sensors and actuators. They are usually federated as systems communicating with each other and with the humans over the Internet of Things (IoT), a network infrastructure enabling the interoperability of these devices (Ratasich et al., 2019).

Serpanos and Wolf, on the other hand, emphasize the importance of safety and security, traditionally the main subject of two different engineering and computer science disciplines. Safety relates to eliminating accidents and losses, while security is historically viewed as a data or communications security problem and is usually conducted by computer scientists. Thus, advances in CPSs and the Internet-of-Things (IoT) require us to take a unified view of safety and security (Serpanos & Wolf, 2018).

The discussions carried out so far can be summarized in a single diagram in Figure 5 below, as suggested by Sisinni et al., 2018.

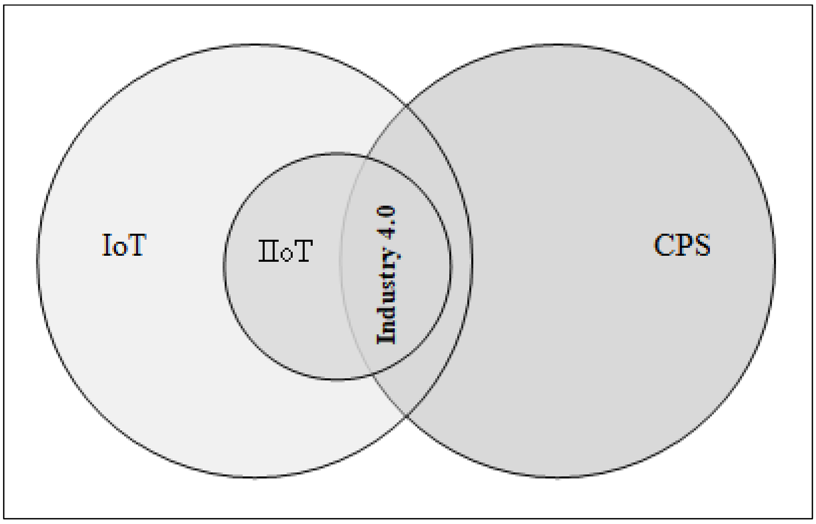


Figure 5 Intersections of IoT, IIoT, Industry 4.0, and CPS
Source: Sisinni et al., 2018 *(redrawn by the author)*

Discussions in this section reveal that cyber-physical systems are not a new phenomenon but have become open to data communication thanks to IIoTs.

2.3. IIoT System Components

This section aims to clarify the current technical underpinnings of IIoT systems in their recent form. The content is vital since IIoT and IoT technologies are fast changing. Therefore, the concept will be presented in technical detail and with concrete examples in this section.

According to Bali et al., the must-have components in a most basic IIoT system can be listed as IoT/IIoT devices, storage, and user interface (Bali et al., 2020). Additionally, Bellavista and Foschini underline the importance of gateways and state that in the basic structure, the gateways must join this system to raise the security posture. So they also add the gateways to the basic IIoT system and name the structure as **the first evolution wave** (Bellavista & Foschini, 2020; Serpanos & Wolf, 2018).

Based on the definitions given in this section so far, the components building a basic IIoT system can be illustrated as in Figure 6 below:

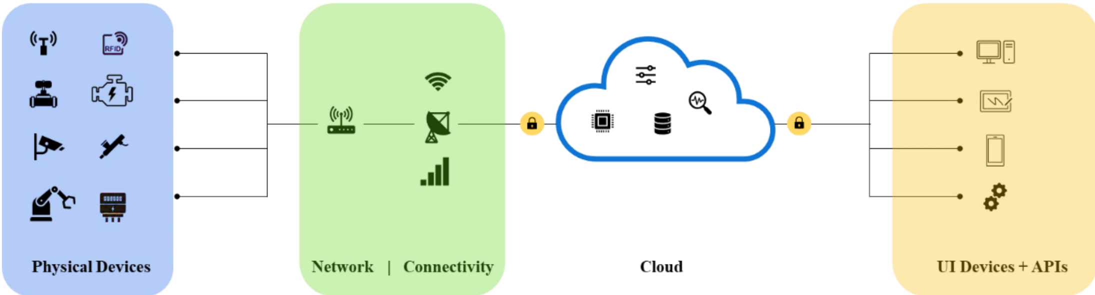


Figure 6 Components of a primary IIoT System
Source: Boyes et al., 2018 *(adapted and redrawn by the author)*

In an advanced IIoT structure, which is named **the second evolution wave** by Bellavista and Foschini, Fog Computing and Edge Computing components are also included in the system (Bellavista & Foschini, 2020; Cao et al., 2019). These technologies will be discussed in the other sections. Each component that makes up the simple structure will be briefly introduced in the following subsections, and real-life examples will be given.

2.3.1. IIoT Physical Devices

Amalraj, Banumathi, and John define an IoT/IIoT device as hardware equipment used to collect data from the physical environment and state that The IIoT device is generally capable of detecting changes in an environment, measuring a physical phenomenon, and transforming it into an electric signal (Amalraj, Banumathi & John, 2019).

Sensors, actuators, accelerometers, gyroscopes, and RFID chips are examples of such components that make devices smart (Thiagarajan, 2016). Objects, light, sound, speed, number, weight, temperature, pressure are examples of data collected by IoT devices (Singh & Viniotis, 2017).

According to Tychogiorgos and Bisdikian, organizations should consider some issues when choosing an IIoT sensor. First of all, the sensor should be selected considering the intended use and ambient conditions. In addition, considering their giant volumes, they should be easily integrated with existing systems and machines and easy to maintain. The sensitivity and accuracy rates of sensors, mainly used in critical infrastructures, should be close to 100%. Finally, the prices should be acceptable (Tychogiorgos & Bisdikian, 2011).

Furthermore, TrendMicro highlights the possible security vulnerabilities with the increase of intelligent devices and states that IIoT adopters have the de facto responsibility to secure the installation and use of their connected devices. In parallel, device manufacturers must protect their consumers when they launch their products, ensuring users' safety and providing preventive measures (TrendMicro Report, 2020).

In parallel to these challenges, Evans and Donnellan expect a radical change in the sensor market in the coming years because of security vulnerabilities, integration problems, high energy consumption, ongoing maintenance, and cost challenges (Evans and Donnellan, 2015). We can see the first examples of this in Norway-based "Disruptive Technologies Company," which emerged with small, wireless, and plug-and-play sensor concepts (Disruptive Technologies Company Website). The next-generation IIoT we mentioned here is given in the example below:

Example-1: IIoT Temperature Sensors

A traditional temperature sensor (on the left side) and the new-generation temperature sensor (on the right side) are given in Figure 7 below to provide a visual idea. The next-generation sensor on the right has no connection requirements. It is sufficient to remove the label on the back and stick it to the equipment where the temperature will be measured.

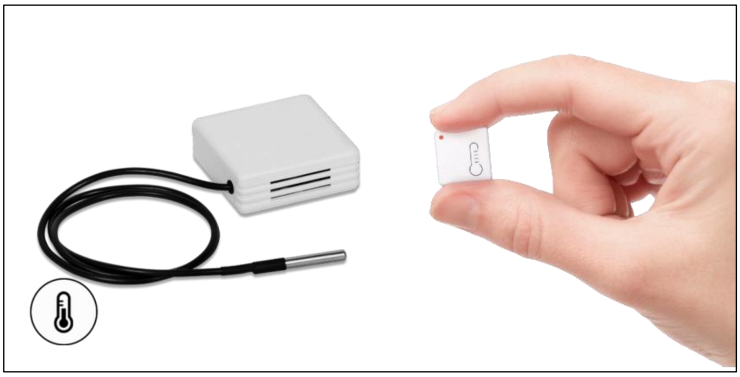


Figure 7 Traditional and new-generation IIoT sensors to measure temperature
Sources: Progressive – IoT Company; Disruptive Technologies *(adapted)*

Example-2: V-Count Ultima AI People Counting Sensor

V-Count AI-based IoT/IIoT sensor, given in Figure 8 below, can perform people counting, gender and age (demographic) analysis, queue management analysis, group analysis, and child-adult analysis with a single device in any indoor environment such as a retail store, restaurant, factory, or cafeteria.

Figure 8 V-Count Ultima AI Counting Sensor *(Image courtesy of V-Count)*

2.3.2. *IIoT Connectivity*

Connection and protocols are among the most talked-about problems in IIoT technology. The connected systems' variety and possible vulnerabilities create interoperability problems between systems (Gebremichael et al., 2020; Perwej et al., 2019; Nicolescu et al., 2018; Serpanos & Wolf, 2018). The communication standards and technologies can be classified into six main groups:

- **Wireless personal area network (WPAN):** WPAN includes three popular wireless sensor network technologies: ZigBee, ISA 100.11a, and Wireless HART. These technologies are based on IEEE 802.15.4, which involves low-rate wireless personal networks (Gebremichael et al., 2016; Cao, Wachowicz & Renso, 2019; Colakovic and Hadzialic, 2018).
- **Wireless local area network (WLAN):** IEEE 802.14.5, Wi-Fi, and Bluetooth are the primary standards and technologies used for communication in IIoT systems (Cao, Wachowicz & Renso, 2019).
- **Cellular network:** Due to its high-speed and high-volume data transmission capability, 5G technology is already a candidate to become the de facto cellular network standard used in IIoT systems (Sisinni et al., 2018). However, 3G and 4G Technologies are used in various projects where 5G is not widely used.
- **Low power vast area network (LPWAN)**: These emerging technologies include SigFox, LoRa, and NBIoT spectrum band, which are used to reduce power consumption and cost of IoT devices and increase reliability and range (Sisinni et al., 2018; Bansal & Kumar, 2020).
- **Satellite network is used for sensors requiring** location tracking and often include GPS technology (Liao et al., 2018).
- **Traditional industrial computer network (Fieldbus):** Fieldbus includes HART and PROFINET protocols. Effective and efficient integration of IIoT with HART and PROFINET is discussed as a significant challenge as many legacy production systems use it (Petrik & Herzwurm, 2020).

In addition to these communication technologies, IIoT devices use messaging protocols such as MQTT, XMPP, DDS, and AMQP to communicate through interconnected networks. The definitions and application areas of these protocols are as follows (Soni & Makwana, 2017; Gebremichael et al., 2020; Zeman et al., 2017):

- *MQTT (Message Queue Telemetry Transfer)* is a machine-to-machine (M2M) protocol used to transmit data to the servers. The primary purpose of MQTT is to manage IoT devices remotely. MQQT is generally preferred in city management, underwater lines, power lines, consisting of small appliances in large networks and organized from a central point. Easy commissioning is its most significant advantage (Soni & Makwana, 2017).
- *XMPP (Extensible Messaging and Presence Protocol)* uses an XML format for instant messaging. Since XMPP is an open protocol, anyone can have their XMPP server on their network without connecting to the Internet. XMPP can be used in applications such as an intelligent thermostat accessible from a smartphone via a web server or a game console with instant messaging between two online players. Since it was developed as a text-based messaging application, it does not require

end-to-end encryption (Soni & Makwana, 2017; Brambilla, Umuhoza & Acerbis, 2017).

- *DDS (Data Distribution Service)* directly connects IIoT devices, unlike MQTT. It does not need any server, and therefore DDS is much faster than MQTT; It can deliver millions of messages to several different recipients in seconds. DDS can also be used to provide device-to-device communication over the bus. It also offers detailed Quality of Service and reliability. DDS is preferred in applications that require fast and reliable communication, such as military systems, wind farms, hospital integration, medical imaging, asset tracking systems, and automotive testing and security (Soni & Makwana, 2017).
- *AMQP (Advanced Message Queuing Protocol)* is an open standard application layer protocol that sends transactional messages between servers. As a message-centric middleware, it can handle thousands of reliable queued transactions. AMQP focuses on monitoring and delivering messages as intended, regardless of errors or reboots. AMQP is primarily used in applications that need to communicate and verify with back-office data centers such as banking, insurance (Soni & Makwana, 2017).

All the protocols listed above are uniquely applicable to different operating scenarios. Any protocol for IIoT application development can be chosen based on its pros and cons. The application's quality of service, security, and reliability are the main factors to be considered when selecting these protocols.

2.3.3. IIoT Gateways

Bellavista and Foschini emphasize the importance of gateways and add that gateways can perform critical tasks, including data buffering, efficiency, data aggregation, data filtering, security, scalability, service discovery, and geo-localization (Bellavista & Foschini, 2020).

Perwej et al. point out that when the complexity of these networks rises to hundreds & thousands of connected things or nodes, preserving the system's quality and reliability will be an elementary problem to consider. In that scenario, modifications will be required in the communication protocols (Perwej et al., 2019). As McKinsey & Company stated in its report published in 2021, interconnected devices use gateways to receive universal communication protocols. Generally, security is not considered sufficiently in developing such protocols and gateways (McKinsey & Company Report, 2021).

On the other hand, referring to ITU's reference model, Serpanos and Wolf declare in their studies that IIoTs can theoretically communicate with each other *without* gateways. As indicated in Figure 9, the model considers three methods of communication, based on the employment of gateways (G) and the use of the communication network (CN). Devices (T) can communicate without using gateways directly, over local networks, or through the communication network, or they can communicate over the communication network exploiting gateways (Serpanos & Wolf, 2018).

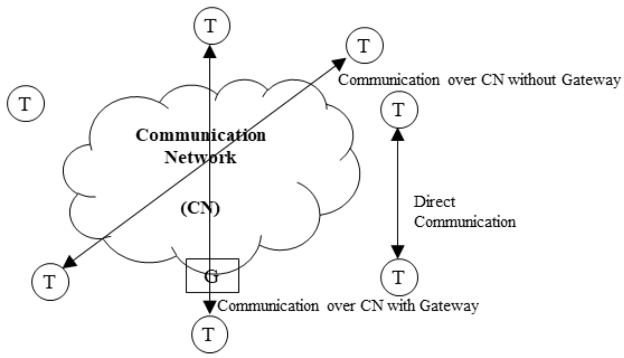


Figure 9 Communication Methods for IoT/IIoT Devices
Sources: Serpanos & Wolf, 2018 *(adapted)*

The above discussions reveal that gateways are not mandatory in an IIoT structure. However, as they enable security mechanisms and provide interfaces to integrate into the existing systems, they should be considered in the system.

2.3.4. Cloud Function

The cloud is a parallel and distributed system described as an application execution and data storage model. Cloud function facilitates the advanced analytics and monitoring of IoT/IIoT devices to shorten the execution time, reduce costs, and reduce energy consumption (Bali et al., 2019).

According to the Industrial Internet Consortium, thousands of devices in a typical IIoT system communicate with a cloud system and store data in the cloud. Using shared third-party service providers creates some trust boundaries that can affect security and privacy; therefore, the information must be protected for security and privacy. Data flowing into control systems must be sufficiently secured to maintain the security and flexibility of physical processes. For example, stolen credentials could allow attackers to remotely control physical infrastructure and simultaneously facilitate attacks against many vendors' customers. Furthermore, attacks against other cloud clients or the platform can spread, allowing attacks against the process owner (Industrial Internet Consortium, 2016).

In the phone interviews, particularly in Turkey and the Middle East, professionals working in the manufacturing industrials said that one of their most considerable reservations about using IIoT technology is that their data goes to the cloud. A majority of the participants said that it is a significant risk for the sensitive data of their businesses to go to the data centers of cloud technology providers outside the country/region borders such as Google, Amazon, Microsoft. This problem will be discussed in more detail, mainly when the results of the qualitative research are explained.

2.3.5. IIoT Device User Interfaces

Patel and Patel define the user interface as a visual representation of measurements in a given context and interaction with the user (Patel & Patel, 2016). According to Bali et al., the user interfaces are the visible and tangible parts of the IoT/IIoT system, allowing users to communicate and monitor their activities in the services they currently subscribe to (Bali et al., 2019).

Brambilla et al. point out that user interfaces can play a crucial role in accepting IoT solutions by final adopters (Brambilla et al., 2017). In this case, the user interface and workflow should be simple enough for an industry professional to define, update and monitor security status accordingly. (Industrial Internet Consortium, 2016).

Example: User Interface of V-Count Business Intelligent Platform

The user interface of the cloud-based business intelligence platform offered by V-Count to its customers using IIoT sensors is given in Figure 10 below:

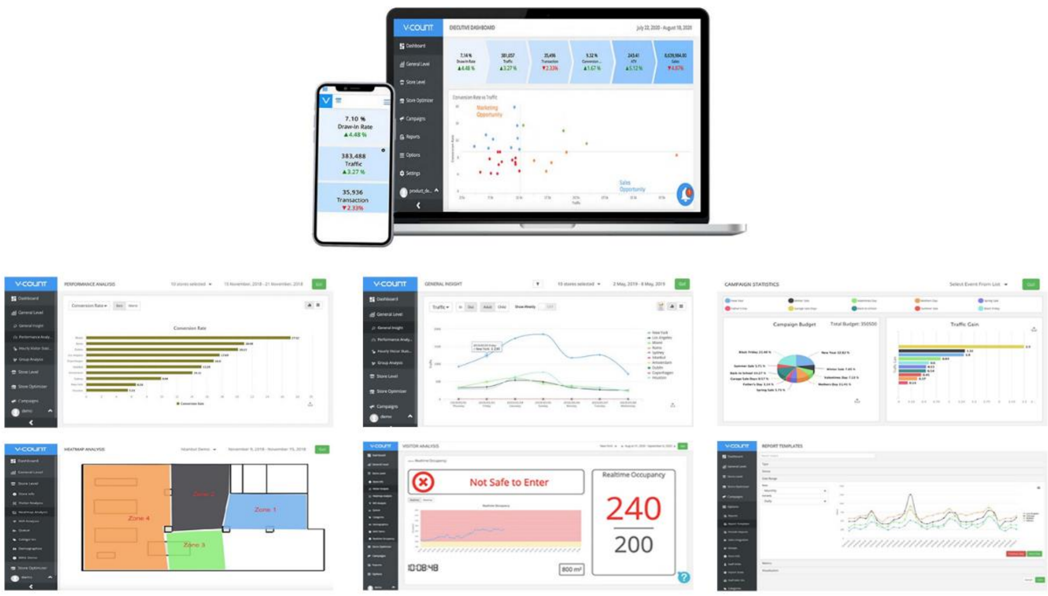


Figure 10 UI screenshots of the V-Count business intelligence platform
(Images courtesy of V-Count)

2.4. IIoT-enabled Emerging Technologies

According to Microsoft's report in 2021, artificial intelligence, edge computing, and digital twin are the leading technologies that increase in value with IIoT (Microsoft & Hypothesis, 2021). For example, an IIoT combined with AI can be a perfect solution to predict the operational process and make decisions (Reddy & Sujith, 2017). On the other hand, thanks to edge calculation, many operations can be done locally, and thus, the cloud system is not overloaded (Shi et al., 2016). Thanks to the digital twin, field and employee safety can increase considerably (The Industrial Internet Consortium Journal, 2021).

However, according to the same report, these technologies remain mainly in the PoC stage due to complexity, lack of infrastructure, and costs (Microsoft & Hypothesis, 2021).

In the following subsections, IIoT enabled emerging technologies will be presented.

2.4.1. Machine Learning Technologies within IIoT Context

Today, human-based data production produces more than 10 times the data produced by traditional working life, and sensor-based data production produces data as fast as 50 times. According to IDC's report, the amount of data created in 2020 alone has exceeded 64ZB (IDC report, 2021).

Humans alone can't cope with the analysis of so much data. Here is the point where artificial intelligence comes into play. The most significant contribution of AI to IIoT is making sense of collected data. The data collected thanks to AI gains meaning in milliseconds with historical data, the root causes of the events can be detected instantly, and future predictions can be made (Khalil et al., 2021).

However, there is the problem of machine learning. Installing the AI system in an IIoT network is no easy task. AI has to spend a lot of time with sensors and objects; therefore, each project has unique characteristics (O'Keefe et al., 2020). For example, the performance of a system deployed for demographic analysis in one country may be different in another country since the phenotypes of people can vary significantly from country to country.

The same situation can be experienced in other cases where AI technology is applied together with IIoT, such as automatic plate recognition systems or automatic product counting and maintenance prediction in a production line, security infrastructures, and machine parks (Sahu et al., 2020). This learning process can be pretty typical for the manufacturer and integrator, but it means patience on the customer's side. Customers want to get the return on their investments immediately; they often cannot tolerate the system to settle in 5-6 months and up to 24 months, depending on the system's complexity to be applied.

The following application example shown in Figure 11 can be given for AI to work with IIoTs. The license plate of a vehicle traveling at a speed of 130-150km/h can be recognized from distances up to 300 meters with sensors mounted on a car at the same traveling speeds. More importantly, this recognition can be done for up to 100 vehicles simultaneously, depending on processors' capabilities. The content of the plate read can be instantly compared with the databases, and necessary information can be given to the officials.

Figure 11 Automatic License Plate Recognition
Source: Ekin Technology (*Image courtesy of Ekin Technology)*

The process of license plate recognition is as in Figure 12 below:

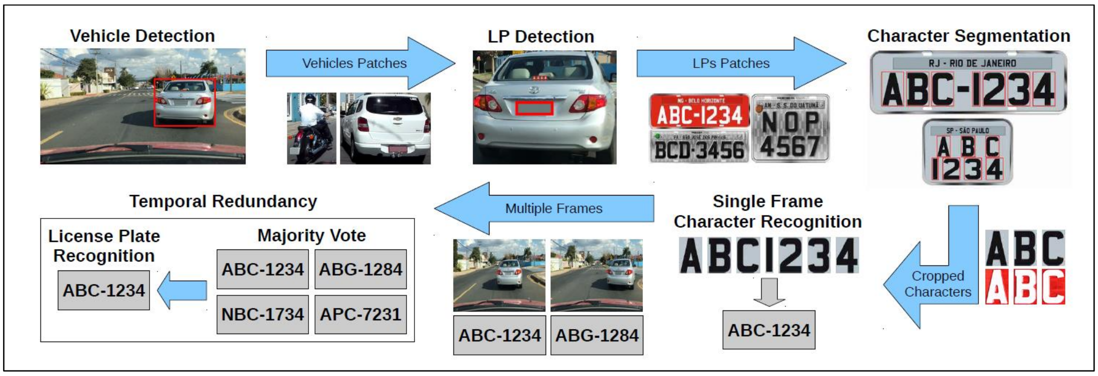


Figure 12 Automatic Plate Number Recognition Process
Source: Laroca et al., 2019

License plate recognition systems generally have four stages: capturing the image, locating the LP frame in the acquired image, segmenting each character within the detected LP, and classifying each segmented alphanumeric character (Laroca, 2019; Sahu et al., 2020).

2.4.2. Digital Twins within the Context of IIoT

Annicchino et al. define the digital twin as a concept that combines different technologies (IoT, artificial intelligence, machine learning, and software analytics) to realize a digital copy of a physical entity, animate or inanimate. This approach aims to monitor, control and simulate production environments in the most realistic way possible (Annicchino et al., 2018). Likewise, Gilchrist states that the "digital twin" concept is vital in the production and the future of the Industrial Internet, allowing Big Data analytics to identify the risks tested in a virtual twin machine before manufacturing (Gilchrist, 2016).

The digital twin can be used specifically for the following applications:

- **Future changes in the physical system are predictable:** Simulation-based analysis of operational data and maintenance from the digital twin improves system performance and contingency planning and supports optimization of the operation, including meeting the requirement and identifying root causes. It would be sufficient to place the digital twin in the control loop to change the parameters of a physical system to predict future changes and handle unpredictable, dangerous events (Singh et al., 2019; Sopapradit & Yoosomboon, 2019).

- **The model of the system can be validated with real-world data:** The system's interactions with the environment and the data of the operational environment can be integrated into the digital twin to make predictions and decisions and validate their models (Kumar et al., 2020).

- **Easier and faster decisions for the users:** Once the data is integrated into the system, the digital twin of a physical object can be used in the situation analysis mode to create appropriate decision supports and notifications to physical system operators (Sopapradit & Yoosomboon, 2019).

2.4.3. Edge Computing and Fog Computing within the Context of IIoT

According to Karim Arabi, the scientist that used the term Edge Computing at the IEEE DAC seminar in 2014, cloud computing works on big data, while Edge Computing works on "instant data," which is real-time data generated by sensors or users (Arabi, 2014).

Due to the increasing demand for low-latency-based computations in the massive-scale IIoT networks, traditional cloud computing-based solutions might not suit industrial applications. Edge Computing has emerged as an encouraging technological solution that performs some of the computation, resources, and services at the network's edge, minimizing latency and providing high network efficiency and system reliability (Porambage et al., 2018; Stankovski et al., 2020; Kumar et al., 2020).

Shi et al. point out the rationale behind Edge Computing and state that more than 45% of the data generated in an IIoT ecosystem will be processed and analyzed at the edge of the network in the future (Shi et al., 2016). On the other hand, according to Lopez et al., data can travel between different distributed nodes connected over the Internet in Edge Computing. Thus, unique cloud-independent encryption mechanisms may be required. End nodes can also be resource-constrained devices, limiting the choice in terms of security methods. It may also need a shift from a centralized, top-down infrastructure to a decentralized trust model (Lopez et al., 2013).

In contrast, Fog Computing is a mediator between the edge and the cloud computing function handling data filtering. It is also noteworthy that Fog Computing can't replace Edge Computing (and cloud computing), while it can live without Fog Computing in many applications. They see Fog Computing as an impeccable partner or an expansion of cloud computing (Malik et al., 2015).

In their lectures at the University of Bologna, Bellavista and Foschini talk about the benefits of using Fog and Edge Computing in the manufacturing industry. Some of these benefits can be summarized as follows (Bellavista & Foschini, 2020):

- **Increased agility:** This can enable organizations to make quick changes in their production lines and introduce new products.
- **Reduced downtime:** Fog and Edge Computing can reduce downtime by enabling predictive maintenance to avoid costly equipment and provide early detection of problems by receiving data from machines in the field promptly.
- Constantly communicate with security systems and confirm in real-time that there is no problem across the network.
- Automatically shut down compromised equipment or suspend its operation without waiting for a human to respond to an alert.

Based on the discussions in this section, the advanced structure of an IIoT system can be illustrated as given in the following Figure 13:

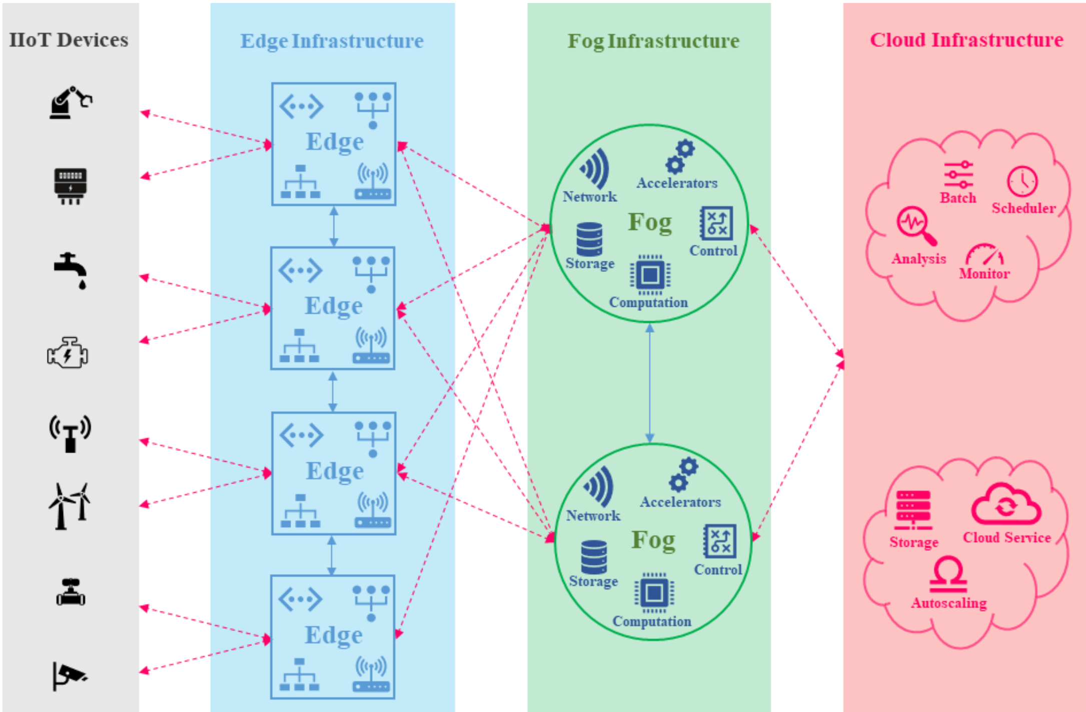


Figure 13 Components of an advanced IIoT System
Source: Cao et al., 2019 *(adapted and redrawn by the author)*

2.5. Benefits of IIoT Technology

According to Perwej et al., IIoT proposes the unique identification and virtual representation of objects as the basis for developing applications and services. They are characterized by massive and self-managed data capture, event transmission, network connectivity, and interoperability. IIoT technology and applications have become the drivers of investment and innovation in many industries, providing valuable benefits to citizens, customers, and industrial end-users in the years to come (Perwej et al., 2019).

Additionally, while the expectation of a mass production company from IIoT, for example, is to increase production and increase quality, a company operating in the oil and gas sector can expect the most workplace safety. Microsoft's recent research on IIoT discloses the different expectations for different sectors as follows:

Table 2 Benefits of adopting IIoTs for various industries

Manufacturing		**Power & Utilities**		**Oil & Gas**	
Quality and Compliance	47%	Smart grid automation	44%	Workplace safety	45%
Industrial Automation	45%	Asset maintenance	43%	Employee safety	43%
Production flow monitoring	43%	Remote maintenance	40%	Remote maintenance	39%
Production plan. & Scheduling	38%	Smart metering	37%	Emissions control	35%
Supply chain & logistics	38%	Workplace safety	37%	Asset and predictive maintenance	35%

Mobility		**Smart Places**	
Quality and Compliance	47%	Smart grid automation	44%
Industrial Automation	45%	Asset maintenance	43%
Production flow monitoring	43%	Remote maintenance	40%
Production plan. & scheduling	38%	Smart metering	37%
Supply chain & logistics	38%	Workplace safety	37%

The main benefits of IIoT systems by addressing these expectations can be listed as follows:

2.5.1. Enhanced Data Collection

According to Pison et al., most current data collection techniques suffer from limitations and passive use design. The IoT rips it out of these spaces and places it exactly where people want to analyze our world. It provides an accurate picture of everything. They also argue that IIoT technology should be seen as a technology stack that takes data from thousands of devices and enables this data to be processed (Pison et al., 2019). Besides, the amount of data collected through devices is no longer limited by the capacity of the systems. Thanks to secure cloud structures, all desired data can be stored in the cloud and processed remotely at any time (Khalil et al., 2021).

2.5.2. Real-time Analytics

Real-time data is mobile information when compared to cloud-based or decentralized. A large data center placed someplace in the world is a cloud and accessed on a need basis. Whereas actual data is communicated synchronously, the operations are happening for these manufacturing industries where data is crucial for success. Integration with IIoT enables companies to collect data from assets and make informed decisions in real-time (Goundar & Bhardwaj, 2021). Similarly, Lee and Lee point out that monitoring and control systems can enable managers and automated controllers to continuously monitor performance in real-time, anywhere, anytime, with data collected on equipment performance, energy use, and environmental conditions (Lee & Lee, 2015).

Real-time analysis capability provides excellent benefits in healthcare and autonomous vehicle applications requiring instant actions. For example, with the data collected from the autonomous vehicle, possible accident hazards and what's happening around the car can be determined much more quickly and easily (Khalil et al., 2021). Anawar et al. emphasize the necessity of calculating fog for real-time analysis. Thanks to the micro clouds environment, the cloud system's burden, where data silos are stored, is lightened (Anawar et al., 2018). Venanzi et al. also agree with this proposal, emphasizing the importance of fog and edge calculation. Especially in the production sector, the flexibility in production where the fog and edge computing technologies are combined increases the downtime of the machines noticeably (Venanzi et al., 2020).

2.5.3. Better Facility Management and Visibility

Facility management and visibility are the interconnectivity of nearly all the systems in communication and with personnel via interface while keeping hardware connected. These physical systems are progressively able to compete to control and connect themselves automatically within an information network. Sensors can also monitor alarm vibrations, temperature changes, and other dynamics that can be future reasons for less operational conditions (Goundar, Bhardwaj, 2021). For example, if an equipment component suddenly fails, sensors can find exactly where the problem is and automatically send a service request. But most importantly, thanks to its predictive analytics capabilities, IIoT can tell when equipment will have a problem before it happens to allow predictive maintenance that results in less downtime and much faster troubleshooting, resulting in improved safety (Magomadov, 2020).

2.5.4. Improved Supply Chain

The methodologies in traditional environments for analyzing the data suffer from blind spots and significant accuracy flaws; IIoT technology transforms this problem into a more prosperous and influential interaction with the audience (Chowdhury & Raut, 2019). Particularly for manufacturing industries, IIoT has excellent potential for quality control, sustainability, supply chain traceability, and overall supply chain efficiency (Xu, He & Li, 2014). Moreover, better visibility allows shorter production cycles that respond quickly to customer demands, addressing numerous regular business and operating challenges such as increased competition worldwide and rising production costs (Seetharaman et al., 2019).

2.5.5. Optimization and Improved Quality

IoT unlocks critical operational efficiency in the data world; the sensors collect, analyze and aggregate business data and other third-party contingency or confidential data from different stages of the business lifecycle. This data includes the raw materials of typical sensor readings that result in the final stage at the early stage (Chowdhury & Raut, 2019). The data collected can offer enormous possibilities to support decision making, efficiency, productivity, product quality, and minimize production costs (Sandrić & Jurčević, 2018).

2.5.6. Reduced Costs and increased Revenue

The consensus in the OT world is that if it works, there is no need for maintenance. Machines run until they fail, and the fact that eliminating the problem can significantly exceed the cost of proper care is often overlooked. Thanks to IIoT, equipment maintenance and repair costs are reduced considerably (Pizon et al., 2019).

Reasonably, each sector's benefits from IIoT technology are different. In this section, the benefits for various sectors have been examined to compare with the research results.

2.6. Challenges of IIoT Technology

Within the scope of this study, a very detailed examination has been performed to identify possible challenges that may hinder the adoption of IIoT technology. We used the following keywords to identify the relevant articles, conference proceedings, and published company reports that studied the past, current, and future challenges of IIoT technology. "barriers *or* obstacles *or* challenges *or* problems *or* pain points" AND "Industrial IoT *or* Industrial Internet of Things."

As a result of these studies, 42 publications that previously studied various problems in IIoT technology will be examined. The complete list of these publications is cited and given in Appendix A.

Based on the literature research, significant challenges of IIoT technologies can be listed as follows:

Table 3 Classification of reviewed publications

IIoT Challenges	Frequency in the Publications
Security issues	41
Interoperability problems	19
Integration problems with the legacy system	16
Reliability issues	15
Privacy issues	11
Lack of standardizations	9
Heterogeneity	7
Others (problems in IT/OT convergence, lack of qualified skills, costs, maintainability, manageability, operability, usability)	17

These problems can be grouped and classified as follows:

Table 4 Classification IIoT challenges

IIoT Challenges *(classified)*
Compatibility problems (interoperability, integration, standardization, heterogeneity issues)
Trustworthiness (safety, security, privacy, resilience, reliability issues)
Inadequacies of the stakeholders (structural complexity)
Lack of qualified skills (usability and manageability associated with lack of skills)
Financial Issues (Entry costs, recurring fees)

2.6.1. Compatibility Problems and Lack of Standards

According to Gartner's report, announced in 2017, 85% of big data deployment projects such as AI and IIoT fail to pass the preliminary stages because the appropriate amount of data for testing cannot be found. The report shows that the biggest reason for this is the necessity of seamless integration to collect big data from hundreds of different assets even to test the system (Gartner Report, 2017). According to another survey conducted by IoT Nexus, 77% of IIoT professionals see interoperability as the biggest challenge of IIoT (IoT Nexus Survey, 2015). The production environment is full of machines and protocols that are not yet interconnected and often not interoperable (Gravina et al., 2018). At this point, it is undeniable that IIoT system providers reduce the value of IIoT technology in customers' eyes while trying to create their standards and, more importantly, dictate these standards to each other. However, common security standards that have been studied for many years by IEC, NIST, and ISO are easily applicable in an IIoT project. Some of these standards include IEC 62443 to improve cybersecurity posture, ISO 27001 to take overall control of information security, NIST 800-53 (Rev 4 and 5) to control baselines, NIST 800-82 (Rev 2) to secure control systems, and industrial internet security framework (IISF) (Dhirani et al., 2021).

Jangid and Chauhan (2019) define interoperability as the systems' ability and components to communicate, regardless of manufacturers and other specifications. However, as the IIoT system must interconnect billions of heterogeneous objects over the Internet, offering a flexible layered reference architecture is crucial for standardization and regulation organizations (Al-Fuqaha et al., 2015).

However, as the IIoT applications handle substantial data traffic, interoperability and heterogeneity have become significant challenges in IIoT project implementations (Daji et al., 2020; Parpala & Iacob, 2017). Li et al. highlight the necessity of many IIoT devices to be connected through a communication technology to communicate, disseminate, and collect vital information with other intelligent networks or applications (Li et al., 2018). On the other hand, integrating IIoT devices into legacy systems also presents enormous challenges. Such systems often have their standards, and in this case, it may not be possible to get out of the way. Another critical point is that these systems continued their lives closed to the outside world until the day of connection. Therefore, integration studies can be very long and costly, and after so much trouble, it may be decided to change the system entirely or not continue the project (Bekara, 2014).

These discussions and our survey findings reveal that standardization will soon play a more critical role, given the growing need for IIoT solutions interoperability with the growth of the IIoT ecosystem. Companies have been creating strategies and solutions with various platforms and technologies until now. However, this situation can lead to fragmentation of technological solutions, thereby leading to market fragmentation; thus, the compatibility challenge will be further evaluated with the industry experts within the scope of this study while carrying out qualitative and quantitative research.

2.6.2. Problems in Trustworthiness

Due to the different security understandings of IT and OT functions, the Industrial Internet Consortium has classified all security issues under trustworthiness. For example, security, reliability, and privacy are essential requirements in IT function; safety is not considered. Even resilience is considered when business continuity is at the forefront (Industrial Internet Consortium, 2016).

However, safety is vital in the OT function. Reliability and resilience are also two other necessary characteristics to avoid downtime on the production line. Security is more physical security. Until now, the machines on the production line have been closed to the outside of the world. Therefore, cybersecurity has remained a "nice to have" option for OT professionals (Industrial Internet Consortium, 2016).

Fraile et al. also point out the convergence of IT and OT functions and state that the reliability requirements of the systems increase exponentially; therefore, the STRIDE threat model should be applied to each component in the system in their study (Fraile et al., 2018). The characteristic features required for an IIoT system after the convergence of IT and OT functions are given in Figure 14 below:

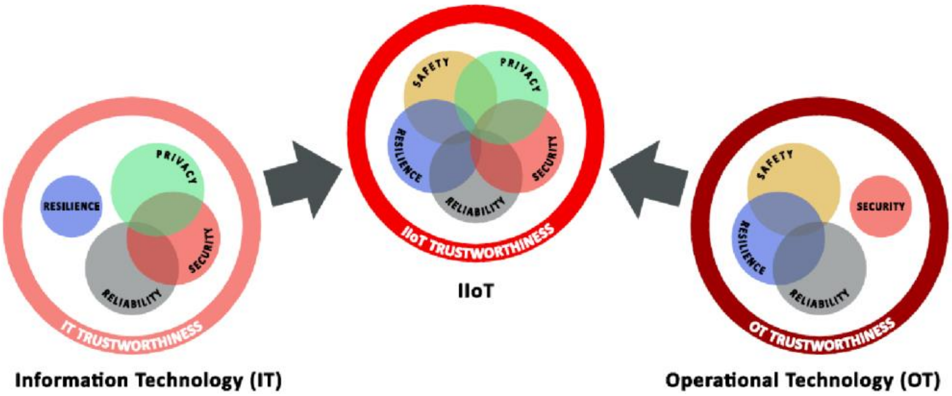


Figure 14 Trustworthiness of an IIoT system after convergence of IT and OT
Source: Industrial Internet Consortium, 2016 *(adapted)*

Referring to the Industrial Internet Consortium's handbook, Nakamura and Ribeiro mention in their studies that IIoT systems have key trustworthiness objectives: privacy, security, safety, reliability, and resilience (Industrial Internet Consortium 2016; Nakamura & Ribeiro, 2018). Likewise, Nicolescu et al., 2018 propose in their studies that safety, security, privacy, reliability, and resilience as the aspects of IIoT systems should be considered across the technological process and throughout the lifecycle of the product and concerning the broader social context in which it operates (Nicolescu et al., 2018).

2.6.3. Safety Issues

Safety is the biggest industry concern, often ignored when Industries adopt IIoT technology (Goundar & Bhardwaj, 2021). IIoT sensors working at critical infrastructures can be vital and even affect the safety of human lives (Thibaud et al., 2018). As seen in many historical cases, industrial sites have been targeted by hackers and subject to cyber-attacks, such as the Stuxnet incidence in which SCADA systems of Iranian nuclear facilities affected millions of dollars in estimated property damage (Forsström et al., 2018).

In the Stuxnet example, IIoT devices were used to run in an internal network and were not open to the Internet; attackers could still exploit the system by placing malicious programs into USB sticks and waiting for someone to plug the USB stick into a system. When the USB stick was plugged in, the virus easily spread through the system until it found SCADA-specific operation systems and caused outages in the Uranium plant. This type of attack can be implemented in any production line where PLCs and IIoT are in use and operation (Mosenia & Jha, 2015).

Stellios et al. conclude the discussions on safety, stating that these intelligent devices can cause even more severe problems when open to the Internet and remote access. Internet access for IIoT devices technically makes it possible for intruders to access every network point (Stellios et al., 2018).

2.6.4. Security Challenges

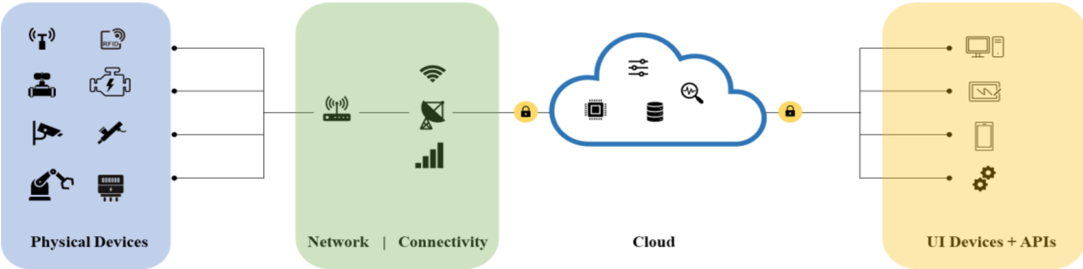
Microsoft and Hypothesis firms have recently announced their reports on IIoT adoption involving more than 3,000 experts in Europe and the US. According to this report, the biggest challenge for experts to adopt IIoT technology was security, with 29% (Microsoft & Hypothesis, October 2021). Additionally, according to Gartner's 2016 IoT Backbone Survey, 32% of decision-making IT leaders such as CIOs cited potential vulnerabilities of physical devices as the biggest obstacle to IoT success after integration (Gartner IoT Backbone Survey, 2016).

Makrakis et al. state that with the advent of IIoT, the big data collected can provide important information to such adversaries. Often these actors can be categorized as foreigners, such as foreign or domestic business competitors who know the antecedents of the target. These actors have the skills to acquire a significant amount of information (such as screenshots, plans, application logic) and often collaborate with insiders. However, they also want to remain as private as possible (Makrakis et al., 2021). As the IT layer moves into the OT side, the attack surface in enterprises has increased exponentially, adding new challenges to the security ecosystem, including (Gajek, Lees & Jansen, 2020):

- Inclusion of all 3rd parties in the ecosystem
- The volume of IIoT devices and large-scale data in circulation
- Previously non-networked devices and IT & OT convergence
- Maintaining currency of patches and software/firmware updates
- Human Factors

Focusing on expanded attack surfaces, Moore et al. state that exposure to cyberattacks is more likely than ever because more industrial users are now accessing all their internet-connected devices and cloud-based services remotely. Until recently, cybersecurity has been focusing on a limited number of endpoints. With the advent of the Industrial Internet, security has to expand its focus to include the physical and virtual worlds at scale (Moore D. et al., 2003). For example, the adoption of the cloud by IIoT will bring many new security challenges, especially data management, access control, identity management, complexity scaling, compliance issues, and legal issues (Cook et al., 2018).

Based on the above discussions, the possible attacks in the IIoT ecosystem can be classified under four main headings, including physical attacks, network attacks, data attacks, and software attacks. IIoT system-specific attack types are shown in Figure 15 below for each component:



Physical Attacks	Network Attacks	Data Attacks	Software Attacks
• Sensor Spoofing • Reverse Engineering • Tampering • Malicious Code • RF Interference/Jamming • Fake Node Injection • Sleep Denial Attack • Side-Channel Attack • Permanent DoS	• Traffic Analysis Attack • RFID Spoofing • RFID Unauthorized Access • Routing Information Attacks • Selective Forwarding • Sinkhole Attacks • Wormhole Attack • Sybil Attack • Man in the Middle Attack • Replay Attack • DoS/DDoS Attack	• Cloud Malware Injection • Authentication Attacks • Data Inconsistency • Unauthorized Access • Data Breach	• Virus, Worms, Trojan Horse, Spyware, and Adware • Malware • Mobile Device Attacks

Figure 15 Possible Attacks in an IIoT System
Source: Sengupta, Ruj & Das Bit, 2020; Panchal, Khadse & Mahalle, 2018; Ankele et al., 2019; Ahemd, Shah & Wahid, 2017; Padmavathi & Shanmugapriya, 2009; Mosenia & Jha, 2016

Khan and Khan point out the targeted attacks on organizations and state that IIoT technology has enabled the oil and gas industry to gain potential benefits such as improved efficiency, lower operating costs, and higher productivity. At the same time, this situation puts critical infrastructures into the fire, making them a primary cyber-attack target led by Advanced Persistent Threats (APT) (Khan & Khan, 2017).

Having so many security risks across the IIoT network is frightening, and solutions must be explored. Literature research on security concerns shows that security can be one of the most significant barriers to IIoT technology adoption.

2.6.5. Reliability Issues

The high accuracy of output in an IIoT system is the success of all components end-to-end (Kim & Dang, 2020; O'Connor & Kleyner, 2012). Suppose the devices in the field measure with high accuracy and the data does not face any problems during transmission and processing. In that case, the analyzes are done correctly, and the necessary actions for possible corrections and improvements are taken correctly (Moore et al., 2020). To state the opposite of this situation, for example, if there is a faulty device in the system and it makes wrong measurements, the reliability will be minimized, decreasing the adoption rate.

A small mistake won't crash a system in a disconnected world, but a fault in one part of a hyper-connected system can cause complete disorganization (Lee & Lee, 2015). Therefore, Industrial IoT systems must be robust in their value proposition, simplicity, and reliability (Brody & Pureswaran, 2015). However, It isn't easy to ensure reliability, especially in an Industrial IoT system, as they are heterogeneous and have a multi-layered infrastructure (Sekar, Shah & Athithan, 2020). Regarding IoT devices, if IoT devices break down due to extreme temperatures, humidity, harsh environmental conditions, it will be difficult for users to adopt IIoT technology. Incorrect analyzes can be made due to malfunctioning devices (Thibaud et al., 2018). Still, more than that, in a possible emergency, environmental disasters, loss of life, long-term disruptions with very high costs may occur (Nakamura & Ribeiro, 2018).

On the other hand, Accenture attributes the reliability problem to the lack of standards in its presentation at the World Economic Forum and states that technology and methodology providers need to establish consensus on the parts produced to fill the gaps in the standardizations. Such a consensus is also very important for the reliability and accuracy of the system (World Economic Forum, White Paper, 2017).

The researchers' views on reliability indicate that potential problems with systems or devices pose a significant risk to adopting IoT technology.

2.6.6. Insufficient Resilience

According to Mimecast's Report published in 2020, 79% of organizations experienced data loss due to a lack of cyber resilience preparedness. In addition, although 43% of employees said that the lack of training and awareness on cybersecurity is one of the most significant security gaps, it turned out that only one-fifth of organizations receive security awareness training periodically. (Mimecast Report, 2021). Gajek et al. attribute this to the fact that organizations do not have sufficient knowledge and, therefore, awareness of cyber-resilience (Gajek et al., 2018).

IT Governance Authority of the United Kingdom, 2016 defines cyber-resilience as the ability to prepare for, respond to and recover from cyberattacks. According to the authority, Cyber resilience has emerged over the past few years as traditional cybersecurity measures have failed to protect organizations from persistent attacks adequately. The administration also states that cyber resilience helps an organization protect against cyber risks, reduce financial losses, fulfill legal and regulatory requirements to defend against and limit the severity of attacks, and protect its brand and reputation. In line with UK Authority's statement, Nakamura and Ribeiro also highlight the importance of resiliency to achieve flexibility, adaptability, collaboration, visibility, and sustainability in an IIoT project (Nakamura & Ribeiro, 2019).

2.6.7. Privacy Problems

As the fundamental principle of IIoT technology, any industrial application is enabled by devices that generate, process, and constantly exchange large amounts of data. At this point, Gebremichael et al. underline the methods of data collection and state that if data is not securely collected, processed, and transmitted, user privacy can be compromised, and the firm's competitive advantage disappears. (Gebremichael et al., 2016).

On the other hand, Sadeghi et al. state that privacy in IIoT becomes a more difficult task to achieve as data storage and processing is often delegated to third-party cloud services, thus opening another attack surface (Sadeghi et al., 2015). Tawalbeh et al. highlight the importance of the perceived usefulness of IIoT technology and state that privacy concerns and the potential harm that comes with IoT can be significant in hindering the full adoption of IIoT. It is essential to know that privacy rights and respect for user privacy are critical to maintaining users' confidence and self-assurance in the Internet of Things, the connected device, and the related services offered (Tawalbeh et al., 2020; Nakamura & Ribeiro, 2019). According to Lee and Lee, privacy concerns matter not only enterprises but also the individuals (Lee & Lee, 2015). For example, in intelligent healthcare equipment, IoT devices can also provide large amounts of data about IoT users' location and movement, health conditions, and purchasing preferences, all of which can raise significant privacy concerns.

On top of all these discussions, Trend Micro highlights the regulations and laws that IIoT providers must obey in a report released in 2020. According to the report, IIoT adopters face the challenge of adequately integrating industrial operations with IT, where connectivity and information must be secured. Users' data must be processed under applicable privacy regulations such as the European Union (EU) General Data Protection Regulation (GDPR). While the data collected plays an essential role in generating insights for devices and infrastructures, personal information must be separated from general daily data. Information such as personally identifiable information (PII) should be stored in an encrypted database. Storing unencrypted data in the cloud and other related activities may mean businesses are at risk of exposure (Trend Micro Report, 2020).

2.6.8. Inadequacies of Business Partners

Mc Kinsey & Company recommends companies, in their report dated February 2021, to select a partner instead of a vendor to help implement the IIoT platform and highlights the necessity of following assessments for the IIoT technology adopters before making any decision:

- **Business model.** Does the solution meet the customer's needs? Is scaling possible? Who will own the platform and data?
- **Market readiness.** Is pricing clear? Are there any recurring payments? Is the organization ready for the project?
- **Use-case offering.** Is there a successful implementation by the relevant partner, preferably from the same industry?

- **Development capabilities.** How much is the provider investing in developing the platform further? How is the number of developer resources?
- **Technology.** How suitable is the platform for additional improvements and modifications? Does it offer a detailed and robust security plan?
- **Operations.** How advanced is the management of new releases and updates? How seamless is technical and commercial support?

Kumar et al. state in their studies that from a business perspective, the challenging task in IIoT project implementation is drafting the regulations and standards, which are acceptable by all stakeholders of the ecosystem, including the service providers, network operators, developers, manufacturers, and customers (Kumar et al., 2020). Riasanow et al. summarize the stakeholders of the IIoT system in Figure 16 below in their study, which we believe is very useful (Riasanow et al., 2020):

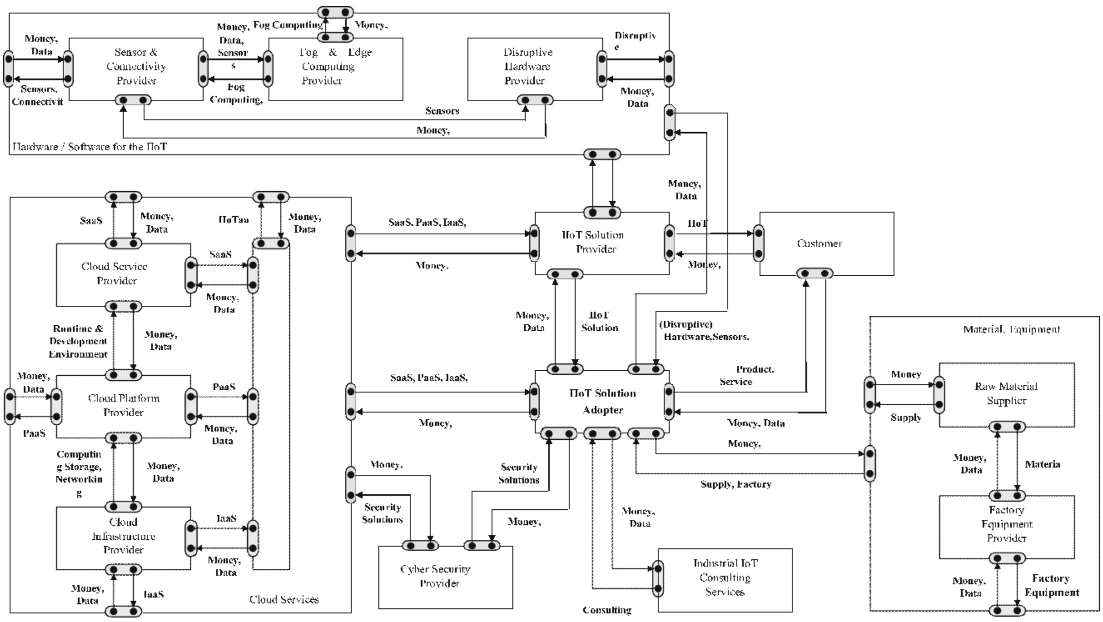


Figure 16 Stakeholders' value chain of an IIoT ecosystem
Source: Riasanow et al., 2020 *(modified for presentation)*

The inclusion of this diagram in our study has two primary purposes. The first is to demonstrate commercial interests among stakeholders in an IIoT ecosystem. Second, it shows how complex the IIoT ecosystem is and needs to be simplified. Frankly, there is considerable heterogeneity among stakeholders.

Eventually, all these privacy issues will be further analyzed in detail in the technology acceptance model proposed within the scope of this study.

2.6.9. Lack of Qualified Skills, Knowledge, and Education

Gartner touches on two critical points in their research conducted in 2021. It is not easy to find data science resources, even with high salaries. Secondly, it will likely take five or more years to improve the skill supply, even as universities increase education in data science (Gartner, Leading the IoT Report, 2021).

In addition to hiring new skills, educating the existing resources and changing the roles of existing resources after the IIoT project is implemented also seem highly difficult. Resistance to change constitutes one of the main challenges facing the adoption of IIoT today. Besides, the fear of job loss in the traditional production environment and creating a new class based on cyber employment is another significant obstacle to implementing IIoT technologies (Rajab, Saxena & Salonitis, 2020; Kusiak, 2018).

In their study, Kamble et al. state that with the commissioning of IIoT projects, changes in job descriptions and the replacement of personnel who have been working on production lines for many years with brand new people are a considerable risk for the future of IIoT (Kamble et al., 2018).

2.6.10. Financial Issues

According to the research carried out by Microsoft and Hypothesis across the Europe region, the number of IoT projects that failed at the proof-of-concept (PoC) stage has increased over the past year. Currently, 35% of Industrial IoT projects experience failure during Trial/PoC, up from 30% in 2020. The most frequently cited reason for failure is the high cost of scaling, which 32% of organizations say is hindering their IoT experimentation. 25% report projects have no net business value or return on investment (Microsoft & Hypothesis, October 2021).

However, the cost is a relative concept (Guggenberger et al., 2021) and varies according to the project's complexity, and firm's economic conditions, purchasing power, and income expectation. Therefore, cost efficiency will also be analyzed in detail within the scope of the research.

2.7. Technology Adoption Models and Methodologies

The most preferred technology-adopted models will be discussed in this section of the study. In this case, it might be good to start with the definitions. *For example*, does accepting a technology mean one's adoption of that technology? *Or* vice versa?

When we search the verbs "accepting" and "adopting" in the online dictionary Merriam-Webster, we come up with the following results:

- *Accepting* is defined as being able or willing to get something or someone, or tendency to look at something or someone with acceptance rather than hostility or fear, or tendency to view different types of people and lifestyles with tolerance and acceptance.
- *Adopting* is defined as accepting formally and putting [something] into effect or taking up [something] and practicing or using [something].

Technology adoption is a process (Arifin & Frmanzah, 2015) that starts with the user being aware of the technology and ends with the user's adoption and full use of the technology. Someone who has adopted technology is likely to replace the piece if it breaks down, finds innovative solutions to fix it, and cannot imagine life without it. Many young mobile phone users have adopted the technology without hesitation. Acceptance, as opposed to adoption, is an attitude towards technology and is influenced by several factors. A user who buys or uses a new technology has not yet adopted it. There are other stages beyond the simple purchase or usage, where acceptance plays an important role. If the user buys a product and then does not accept it, it is unlikely to be fully adopted (Renaud & Biljon, 2008). To give an example from the business world, an organization can impose an in-housed developed CRM application to its employees. An employee's use or consent to use the application does not mean that the employee adopts the application.

2.7.1. Technology Adoption Process

Adoption of technology by its users is, in many cases, a long and arduous process. The technology stakeholders need to know the factors that affect the adoption of the relevant technology or cause it not to be adopted.

The technology adoption process began to evolve when researchers realized that marketers needed to understand potential customers and the factors influencing their purchasing decisions to successfully bring innovative technological products and solutions to the market (Lafreniere et al., 2011; Frambach & Schillewaert, 2002). Early innovation adoption models considered user satisfaction and attitude (Lafreniere et al., 2011; Ramdani & Kawalek, 2007; Venkatesh et al., 2008). Since then, researchers have empirically tested models of adoption, primarily based on theories from the fields of social psychology and behavioral science (Lafreniere et al., 2011; Eckhardt et al., 2009; Ramdani & Kawalek, 2007).

In this context, the technology adoption process is as described in Figure 17 below:

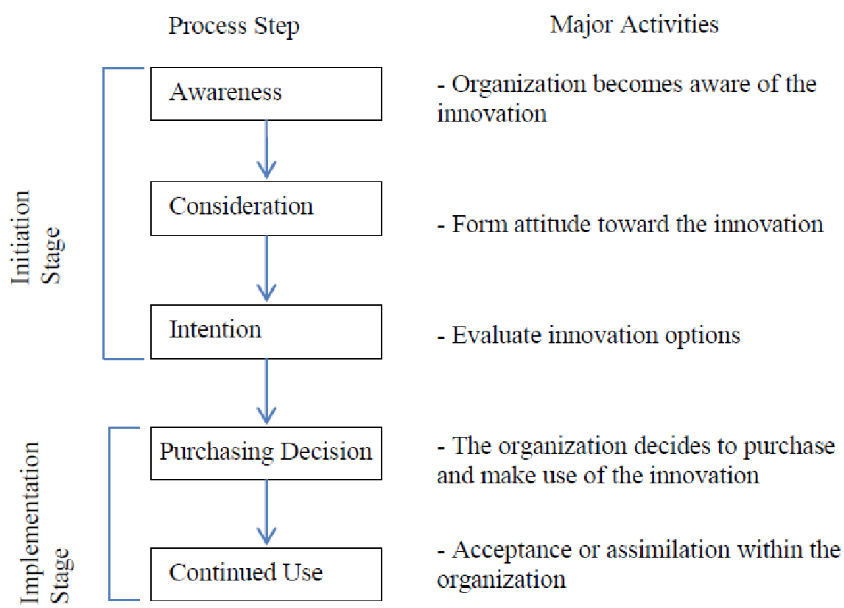


Figure 17 The Technology Adoption Process at the Organization Level
Source: Lafreniere, Hunter & Deshpande, 2011 *(adapted)*

Lafreniere et al. used 'adoption decision' rather than 'purchase decision' in their original work (Lafreniere et al., 2011). On the other hand, Cabral et al. used these two concepts unchangeably (Cabral, Salant & Woroch, 1999). In this case, we have also employed 'purchasing decision' to avoid confusion in the terminology.

2.7.2. Overview of Technology Adoption/Acceptance Models

Numerous studies to date have used various technology adoption models (Junglas & Spitzmüller, 2005; Renaud & Biljon, 2008; Dewan and Riggins, 2005; Lafreniere et al., 2011). According to our research, these models have two common points; firstly, they are all influenced by each other somehow. Secondly, virtually all the models were developed before the millennium era. For example, from 2010 to 2020, 2399 different studies had been published through the "Web of Science" (Al-Emran & Granic, 2020). We also identified that many researchers studying the firms have adopted various models and proposed their models claiming that TAM focuses too much on individuals (or consumers). The interesting point is that there is another group claiming just the opposite. When we read Davis's article published in MIS Quarterly in 1989, obviously we see that all his examples about the model were from the corporate side, and his model can adapt to corporate needs.

The most used adoption models will be reviewed in the following section. In addition to these models, Technology, Organization, and Environment (TOE), the evaluation model used to determine external factors in adoption models will also be introduced.

2.7.3. Innovation Diffusion Theory (IDT)

Developed by Rogers in 1962, the DOI model examines how an idea or product gains momentum in time and spreads or diffuses through a population or a large group. Diffusion results in people adopting a new product, service, idea, or behavior. The critical point to adoption is that the person must perceive the idea, behavior, or product as new or innovative (Rogers, 1963). According to Rogers, adopting a new idea, behavior, or product does not coincide in a social system. Some people tend to adopt an innovation earlier than others. The theory claims that people who adopt a product at different stages during its economic life have different characteristics. Therefore, a manufacturer introducing a new product to the market must do this oversight (Rogers, 1963).

There are five established adopters: innovators, early adopters, early majority, late majority, and laggards. Although most of the general population tends to fall into the middle categories, it is still necessary to understand the target population's characteristics. Different strategies appeal to different types of adopters (Rahman et al., 2020).

The process of diffusion is illustrated in the following Figure 18:

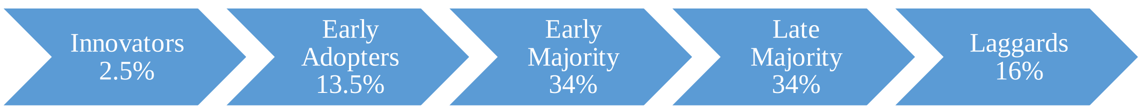


Figure 18 Diffusion of Innovation Theory
Source: Rogers, 1963 *(redrawn by the author)*

2.7.4. Theory of Reasoned Action (TRA)

Considered the ancestor of TAM (Momani & Jamous, 2017), the TRA argues that positive or negative attitudes towards behavior and subjective norms are the two main factors influencing behavioral intention (Ajzen & Fishbein, 1975; Hale, Householder & Greene, 2002).

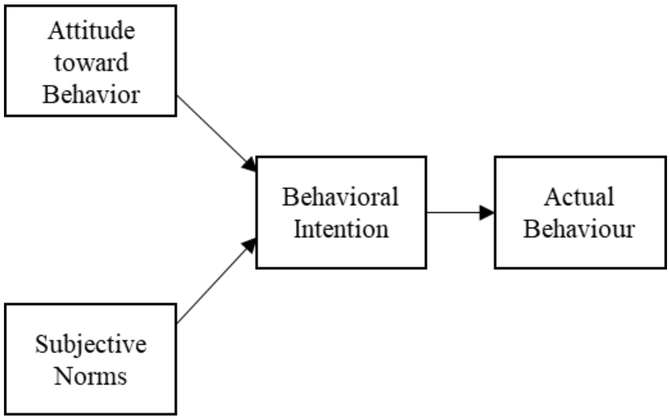


Figure 19 Factors influencing behavioral intention
Source: Ajzen & Fishbein, 1975 *(redrawn by the author)*

According to TRA, attitude towards a behavior is influenced by previous beliefs, evaluations, and consequences. Therefore, the better results individuals expect from exhibiting a particular behavior, the more positive they will be. On the other hand, subjective norms are positively or negatively associated with normative beliefs and individuals' motivations to meet normative beliefs. In other words, the more inspiration individuals have to meet their normative beliefs, the more positive subjective norms they will acquire (Ajzen & Fishbein, 1980; Kocaleva, Stojanovic & Zdravev, 2015).

2.7.5. Theory of Planned Behavior (TPB)

Like TRA, TPB also considers attitude towards behavior and subjective norms as variables that determine innovation adoption. In addition, this theory uses a third variable called behavioral control, which is described as experiencing ease/difficulty in performing the behavior (Ajzen, 1985).

Ajzen describes behavioral control as the perceived ease or difficulty of performing the behavior (Ajzen, 1991). The constraints that are influencing the behavior of a person are given in Figure 20 below:

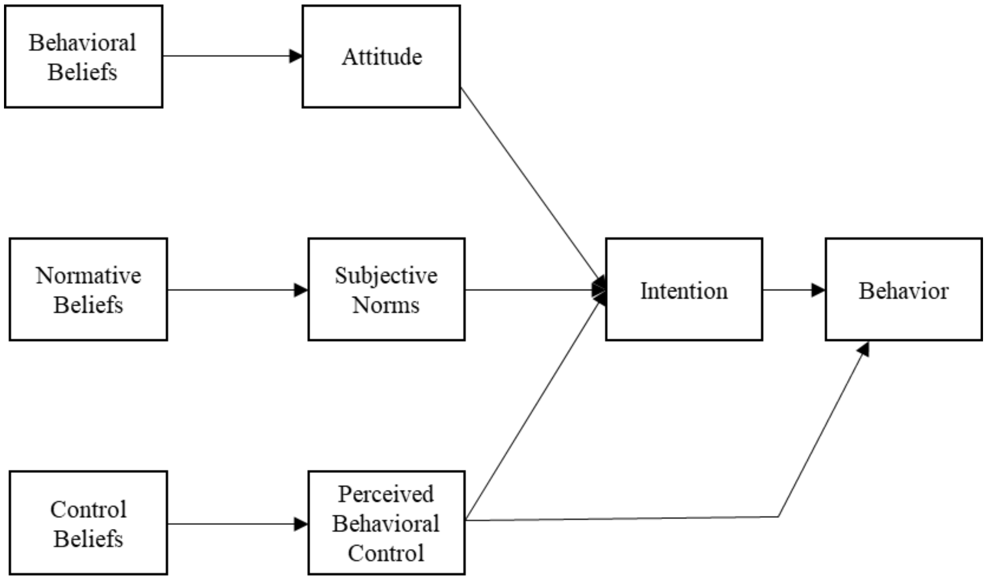


Figure 20 Factors influencing behavior
Source: Ajzen, 1991 *(redrawn by the author)*

The TPB model proposes that behavioral beliefs typically result in a positive or negative attitude towards a particular behavior. On the other hand, normative beliefs result in perceived social pressure or subjective norms, and control beliefs trigger perceived behavioral control.

2.7.6. Technology Acceptance Model (TAM)

Davis (1986) first introduced TAM as an alternative to TRA in his thesis in 1986. However, the version developed in 1989 is more well-known (Davis, 1989).

TAM posits that 'Perceived Ease of Use (PEoU)' and 'Perceived Usefulness (PU)' are the two most important factors that may affect people's decisions to accept or reject the technology. The PEoU factor measures how simply a person perceives a new technology without any effort. On the other hand, PU measures how beneficial a person perceives a new technology to their work or themselves (Davis, 1989). Davis noted in this article that this perceived benefit could be an expectation of salary raise, promotion, bonus, or any other reward (Davis, 1989). Moving further, PEoU also influences PU. For example, when a person encounters a new technology, he may find it more useful and expect a higher benefit if he uses it efficiently. In an organizational context, the more complex a technological solution is, the harder it is for employees to adopt it. That's why solution providers are constantly looking for ways to create simpler user interfaces. Thus, PEoU and PU can positively affect people's attitudes, intentions, and acceptance of new technology. The overview of the TAM model is given as below:

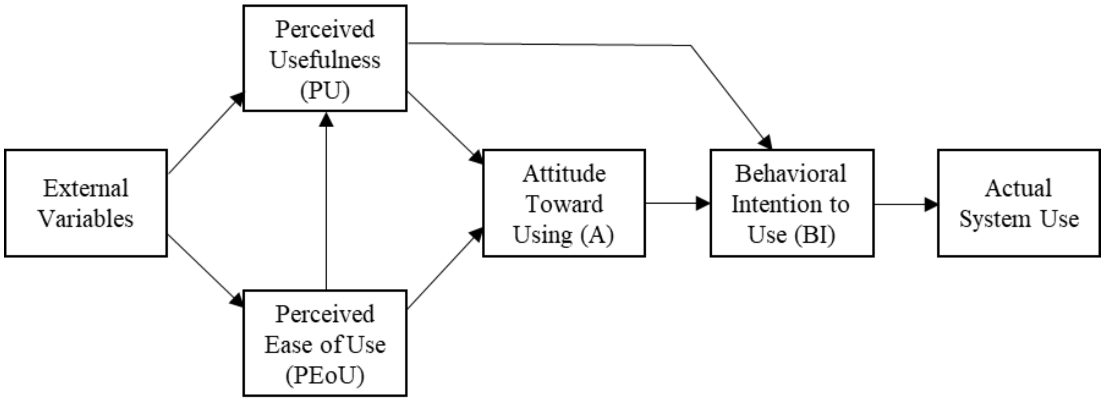


Figure 21 Technology Acceptance Model
Source: Salloum et al., 2019 *(redrawn by the author)*

On the other hand, both PEoU and PU can be both or separately affected by external variables. Yousafzai, Foxhall, and Pallister, 2007 proposed more than 70 external variables classified as organizational characteristic, system characteristics, user personal characteristics, and other variables in their meta-analysis study given as below:

Table 5 External factors that may affect PU and PEoU
(Source: Yousafzai, Foxall & Pallister, 2007)

Organizational Characteristics	**System Characteristics**	**Personal Characteristics**	**Other Variables**
Competitive environment	Accessibility	Age	Argument for change
End-user support	Access cost	Awareness	Cultural affinity
Group's innovativeness norm	Compatibility	Cognitive absorption	External computing support
Implementation gap	Confirmation mechanism	Computer anxiety	External computing training
Internal computing support	Convenience	Computer attitude	Facilitating conditions
Internal computing training	Image/interface	Computer literacy	Subjective norms
Job insecurity	Information quality	Educational level	Situational normality
Management support	Media style	Experience	Social influence
Organizational policies	Navigation	Gender	Task technology fit
Organizational structure	Objective usability	Intrinsic motivation	Task characteristics
Organizational support	Output quality	Involvement	Vendor's co-operation
Organizational usage	Perceived attractiveness	Personality	
Peer influence	Perceived complexity	Perceived developer's responsiveness	
Peer usage training	Perceived importance	Perceived enjoyment	
Transitional support	Perceived software correctness	Perceived playfulness	
	Perceived risk	Perceived resources	
	Relevance with job	Perceived innovativeness	
	Reliability and accuracy	Role with technology	
	Response time	Self-efficacy	
	Result demonstrability	Shopping orientation	
	Screen design	Skills and knowledge	
	Social presence	Trust	
	System quality	Tenure in workforce	
	Terminology	Voluntariness	
	Tribality		
	Visibility		
	Web security		

According to another meta-analysis carried out by King and He, which covered 88 research studies, they found out that researchers have widely accepted TAM as a reliable model for predicting technology acceptance to measure users' perception of technology innovation and probability of acceptance (King & He, 2006).

2.7.7. Technology Acceptance Model 2 (TAM 2)

In this model, Venkatesh and Davis (2000) added new critical determinants to perceived usefulness and behavioral intention, which are the main variables of TAM, and named the model TAM 2 (also known as Extended Technology Acceptance Model). TAM 2 is intended to predict the reasons behind external variables that affect perceived usefulness. The model has two main external elements. The first one is the set of social influence factors, including subjective norm, imagination, and voluntarism. In contrast, the second one is the cognitive tools, including job relevance, result demonstrability, quality of output, perceived ease of use (Davis & Venkatesh, 1996).

According to the model, job relevance is defined as the degree of perception an individual applies to the target system's job, and output quality is defined as the degree to which the system performs work-related tasks.

The elements of the model are given in Figure 22 below:

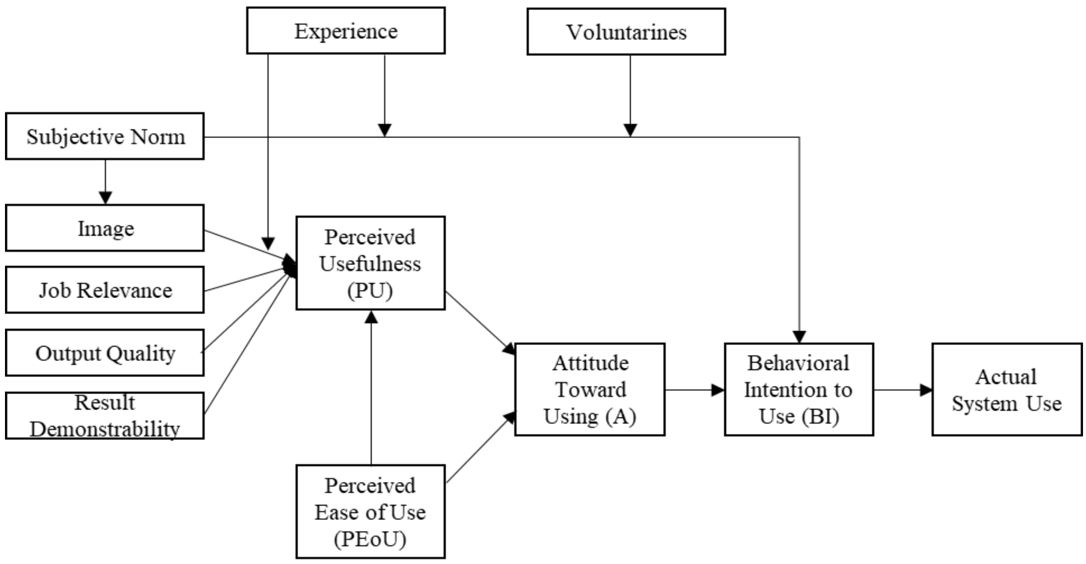


Figure 22 Technology Acceptance Model 2 (TAM 2)
Source: Davis & Venkatesh, 1996 (redrawn by the author)

2.7.8. Unified Theory of Acceptance & Use of Technology (UTAUT)

The Unified Theory of Technology Acceptance & Use (UTAUT) model, based on end-users acceptance and use of technology, is much more advanced and holistic. UTAUT, called the unified model, was formulated by combining elements in eight models (Rahman et al., 2020; Venkatesh et al., 2003; Williams, Rana & Dwivedi, 2015).

UTAUT is a detailed and valuable tool for managers who demand to evaluate the success capacity for new technology talents, and it is a valuable tool for training, marketing, etc. (Venkatesh et al., 2003). The purpose of UTAUT is to explain the user's intentions to use an information system and users' subsequent behavior. UTAUT identifies four main factors and four moderators linked to predicting behavioral intention to use technology and, mainly, actual technology used in organizational contexts (Al-Qeisi, Dennis, Alamanos, & Jayawardhena, 2014; Alwahaishi & Snášel, 2013; Venkatesh et al., 2003).

The model is given in Figure 23 below:

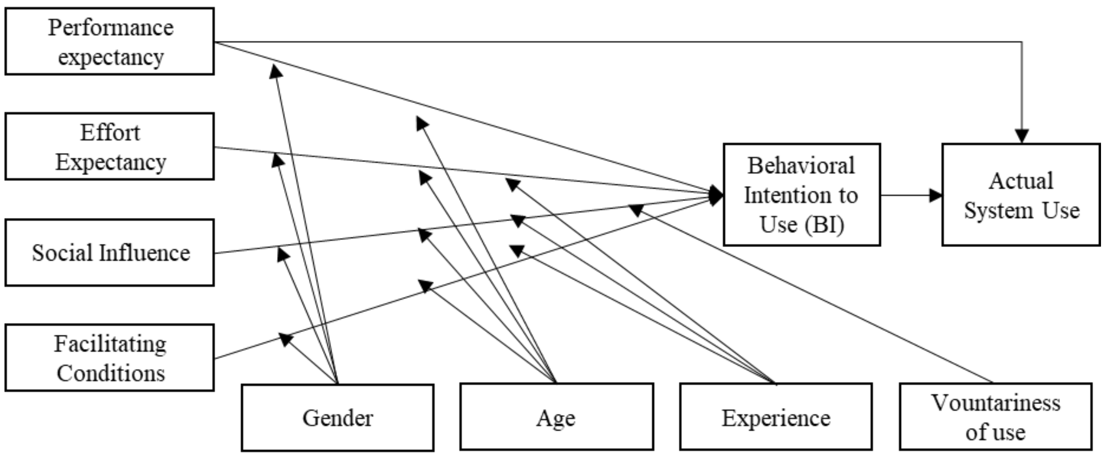


Figure 23 Unified Theory of Acceptance and Use of Technology (UTAUT) Model

Source: Venkatesh, Morris, Davis & Davis, 2003 (redrawn by the author)

The four main factors are described as follows:

- *Performance expectancy* is a person's belief that using innovative devices will help them achieve significant rewards in employment execution.
- *Effort expectancy* is the level of easiness associated with the use of tools.
- *Social influence* is an individual's belief in the respect that others trust that they should use technology.
- *Facilitating conditions* are the belief that the organizational and technical infrastructure exists to support the use of the system.

Gender, age, experience, and voluntariness are structured to balance the four main factors that influence usage intention and behavior.

2.7.9. Unified Theory of Acceptance & Use of Technology 2 (UTAUT2)

So far, models are usually validated by measuring behavioral intention to use rather than actual use. In contrast, UTAUT2 is the all-inclusive and robust model that theoretically has broader applicability, in fact using a wide variety of contextual settings (Rahman et al., 2020).

UTAUT2 is an extended version of the original UTAUT model known as Unified Technology Acceptance and Use Theory 2 (UTAUT2) (Kao, Nawata & Huang, 2019; Chang, 2012; El-Masri & Tarhini, 2017). UTAUT2 extends to UTAUT the complete theory of acceptance and use of UTAUT technology, consisting of three elements: hedonic motivation, price value, and habituation. First, the inclusion of hedonic motivation to support the strongest predictor of UTAUT emphasizes utility. Second, unlike workplace views, users are responsible for costs from a user's perspective, and such charges can monopolize consumer adoption decisions (Kao, Nawata & Huang, 2019; Khatimah, Susanto & Abdullah, 2019; Venkatesh et al., 2012). The price value then complements UTAUT's existing resource metrics to focus solely on time and effort. Finally, bringing together habits will complete the theory's focus on objectivity as the overarching mechanism and primary driver of behavior (Venkatesh et al., 2012; Kao, Nawata & Huang, 2019; Tamilmani, Rana & Dwivedi, 2017).

The model is given in Figure 24 below:

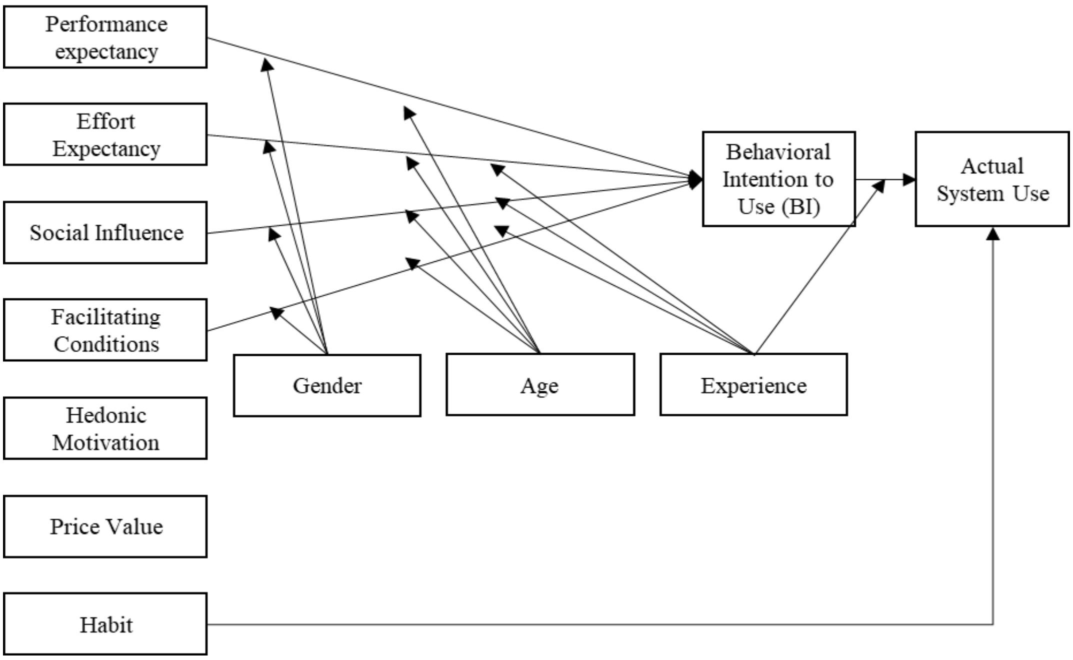


Figure 24 Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) Model
Source: Venkatesh, Thong & Xin, 2012 *(redrawn by the author)*

2.7.10. Technology, Organization and Environment Framework (TOE)

Organizations widely use the model to identify technology characteristics, organizational readiness, and environmental conditions as critical factors in technology adoption (Liu et al., 2011; Kauffman & Walden, 2001; Chatterjee et al., 2021). The TOE framework can be used to determine the external factors of the adopted technology acceptance model (Qin et al., 2020).

The technological context involves internal and external systems already implemented by the organization or available in the market but not used by the organization. The organizational context refers to the company's size, organizational structure, and human resources. The environmental context encompasses factors outside the organization's control, such as competition, partners, and the industry environment (Qin et al., 2020; Drazin, 1991).

The model is given in Figure 25 below:

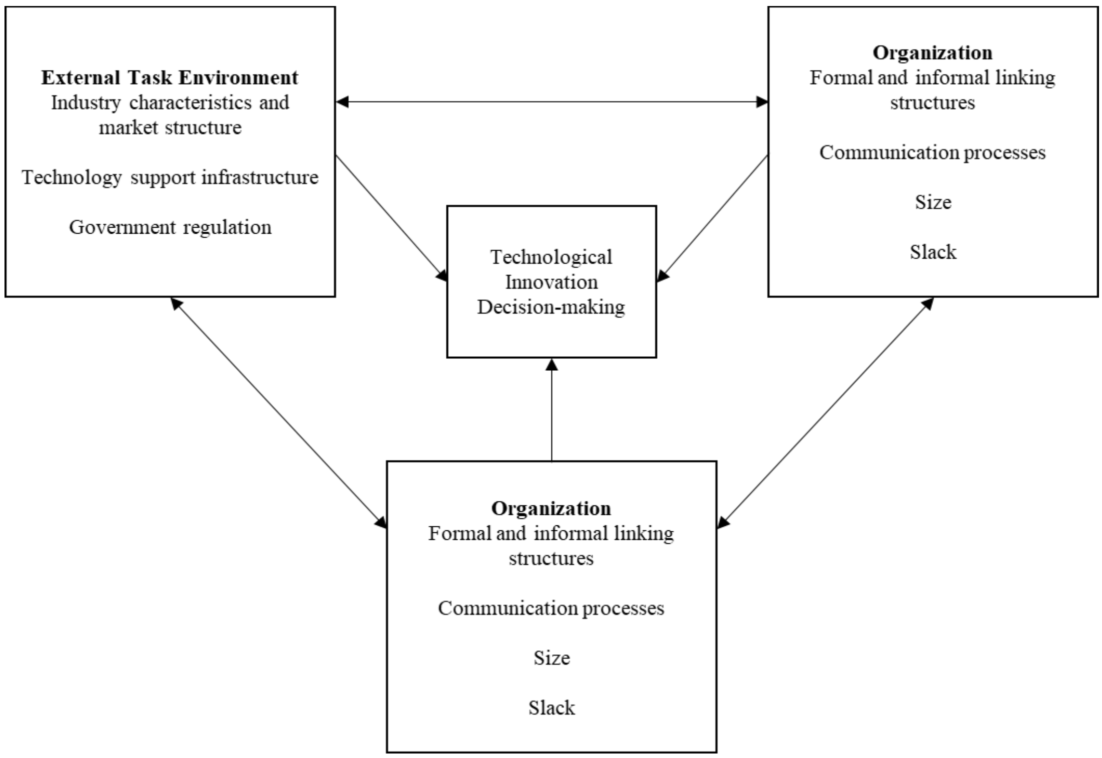


Figure 25 Technology, Organization and Environment Framework (TOE)
Source: Baker, 2011 *(redrawn by the author)*

2.8. A Meta-Analysis of IIoT Adoption Studies

As part of our study, we asked the open-ended question "What does IIoT mean to you" in our survey to determine the keywords we will use. We got answers from 342 people.

We translated the Turkish answers into English and listed the keywords we found below:

Table 6 Identification of keywords

Keyword(s)	Frequency
Sensor	157
Smart	153
Smart sensors	78
IIoT	77
Smart things	66
Internet	56
Things	53
Industrial	44
IoT	24
Internet of Things	6
Industrial Internet of Things	6

After refining the list, we have obtained our keywords as below:

Table 7 Refined keywords

Keyword(s)
Smart sensors
Industrial Internet of Things
Internet of Things
IIoT/IoT
Smart things
Internet-connected smart things
Internet-enabled smart things
Industrial IoT

We combined these with "technology acceptance" OR "technology adoption" by using AND Boolean operator.

2.8.1. Identification of Research Criteria

With our work in this section, the following objectives will be achieved:

- To answer our research question, which was "What is the current state of the technology acceptance of Industrial IoTs by industries in literature?".
- To identify the factors that influence/affect the adoption of IIoT by the industries.
- To understand how research on IIoT adoption has developed over the years.
- To know how, when, and where relevant research has been published
- To review the published studies with a scientific point of view

In line with our criteria, we described our approach as follows:

Table 8 Systematic literature review for acceptance models studied on IoT

Search Criteria	**Including**	**Excluding**
IIoT/IoT technology combined with technology acceptance/adoption model	Review or survey Practical studies Experimental studies Qualitative studies Quantitative studies Studies targeting consumers Studies targeting industries	Non-English Non-research articles Meta-analysis studies Without full-text TAMs without IoT/IIoT Studies on IoT/IIoT, but without TAM Theoretical studies Without samples

2.8.2. Database Selection

We used Google, Google Scholar, Scopus, IEEE Xplore, Elsevier, ScienceDirect, and METU library databases.

2.8.3. Documentation of Systematic Literature Review (SLR) Results

We have added all the studies we have obtained to the spreadsheet with the titles listed below and presented them in Appendix B.

- Author
- Subject
- Published Year
- Country
- Published Organization
- Qualitative *or* Quantitative *or* both
- Consumer *or* Industry Oriented
- Industry *(if any)*
- Model Used

2.8.4. Systematic Literature Review Flowchart

The flowchart of our research with keywords on the adoption of IIoT technology is shown in Figure 26 below:

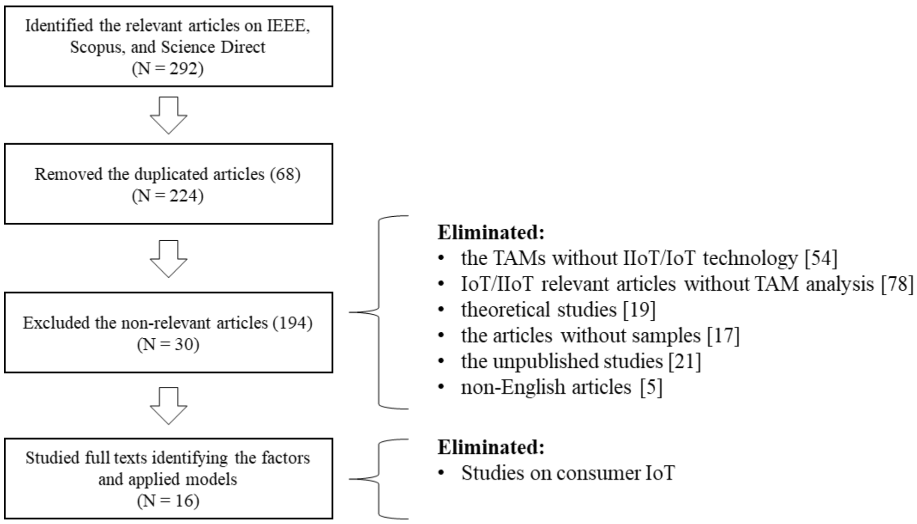


Figure 26 Flowchart of our Systematic Literature Review

2.8.5. Evaluation of Relevant Studies

As a result of our research, we examined 30 published articles or conference papers similar to our subject. We came to the point that the quality of the articles we found, for which we applied a rather strict elimination criterion, was generally good.

What we found interesting in the articles was that almost none of the subject researchers explained how they identified external criteria (such as security concern, lack of trust, management support) that affect the output of the applied model.

The findings are listed as follows:

Table 9 Distribution of technology adoption model studied on IoT and IIoT

Target Audience	**Frequency (N = 30)**	**Percentage**
Consumer	14	47%
Business	16	53%

Table 10 Geographic distribution of technology adoption model studied on IoT and IIoT

Country Distribution	**Frequency (N = 30)**	**Percentage**
India	4	13.3%
Malaysia	4	13.3%
China	3	10%
Saudi Arabia	2	6.6%
Netherlands	2	6.6%
Europe Region, Fiji, Greece, Hungary, Indonesia, Italy, Japan, Jordan, Morocco, Romania, South Africa, Taiwan, Thailand, USA, Vietnam	1 (each) (n = 15)	50%

Table 11 Distribution of technology adoption model studied on IoT and IIoT by year

Distribution of publications by year	**Frequency (N = 30)**
2021	6
2020	6
2019	5
2018	6
2017	3
2016	1
2013	1
2011	1

2.8.6. Sample Size Analysis of the Relevant Studies

We found that the number of samples varied widely in 30 studies. Our analysis understood that the basis of this difference is the country's population where the research was conducted and whether the target audience is corporate users or individual users.

Our findings regarding the number of samples are as follows:

Table 12 Summary of TAM-based publications studied IoT and IIoT

Research Type	Technology	Total	Max	Min	Average	Median
Quantitative	Consumer IoT	13	1356	70	418	378
	Industrial IoT	13	685	72	**224**	140
	All	26	1356	70	366	300
Qualitative	Consumer IoT	1	38	38	38	38
	Industrial IoT	3	43	18	33	37
	All	4	43	18	34	38

As we received answers from **342** people to the survey we conducted in August and September 2021, we say that the number of responses we received is higher than the average of the studies carried on Industrial IoT technology and, therefore, acceptable for a healthy measurement.

2.8.7. The Models Used in the Studies

We focused on 16 studies without distinguishing between consumer or institutional to better analyze the models used.

The list of models used in these studies is as follows:

Table 13 Models used in the studies

Model Used	Frequency (N = 16)
Only TAM	10
TAM combined with TOE or DEMATEL	1
UTAUT	4
TPB combined with TRA	1

2.8.8. Analysis of influencing factors used in models

In our analysis, we have identified many factors used for the same purpose but with different names. The distribution of elements used by the studies is as follows:

Table 14 Influencing factors of the studies focused on IoT

Influencing Factors	**Frequency**
Perceived Usefulness	11
Perceived Ease of Use	11
Compatibility	6
Perceived Risk	6
Social Influence	5
Costs	4
Perceived Trust	4
Experience	3
Self-efficiency	3
Facilitating conditions	3
Job relevance	3
Anxiety	3
Age	2
Innovativeness	2
Gender, company size, interoperability, complexity, stakeholders, company age, culture, competitiveness, management support	1 of each

2.9. Adopted Acceptance Model Theory and Methodology

UTAUT, one of the most used models in research, can be considered a universal model as it combines almost all models and powerfully explains the results (Qin et al., 2018; Taylor & Todd, 1995). However, UTAUT has specific patterns and does not allow the researcher to measure his hypotheses as he wishes. In this context, the UTAUT model is suitable for research where age, gender, experience, and motivation play an important role in technology adoption.

On the other hand, in the target group of our study, the vast majority of the professionals are currently using or likely to use IIoT technology soon and who work in specific sectors and have a particular experience and knowledge. Besides, even if these professionals do not currently use IIoT technology, they have already experienced the technology before, therefore, know very well what IIoT is, its benefits, and current difficulties.

When we look at the Technology Acceptance Model, we see that the model has difficulties measuring the influencing degrees of social factors. In addition, the model does not propose any specific criterion for determining external factors (Qin et al., 2018; Malatji et al., 2020). In our case, there are no social factors. As for external factors, we interpret this situation as the flexibility it has given us.

Eventually, we have decided to use the Technology Acceptance Model in our research, as it is the most widely used, easiest to understand, and provides better flexibility to the researcher. In determining the external factors, we aimed to address the core values and challenges that may affect the adoption of the technology. Benefits and challenges are described in Section 2.5 and Section 2.6, respectively. In addition, as mentioned in Section 2.10, the TOE framework can be used to determine the external factors used in measuring technology adoptions (Liu et al., 2011; Kauffman & Walden, 2001; Chatterjee et al., 2021; Qin et al., 2018). Under these circumstances, we can group the values and challenges faced by IIoT, which we mentioned in the previous sections, as follows:

Table 15 Classified Factors based on TOE methodology

Technology	**Organization**	**Environment**
● IT and OT functions ● Digital transformation strategy ● The situation of using IIoT products and services actively ● Interoperability ● Integration with legacy systems ● Security issues	● Size ● Age of the company ● The sector of the company ● The location of the company ● Position and seniority ● Experience with IIoT ● Management support ● Cost efficiency and ROI	● Relations with the stakeholders, partners, vendors ● Competitiveness ● Standards, policies, regulations

2.10. Summary

So far, we have conducted literature research on IIoT technology and technology acceptance models. In our study on IIoT technology, we examined the components that makeup IIoT technology in detail and identified the benefits and challenges of IIoT technology. We then looked at the acceptance models, in particular, discussing the advantages and disadvantages of each, and determined the model and methodology that we would use.

In the following sections of our study, we will discuss our research methodology, survey structure, and results.

CHAPTER 3

RESEARCH METHODOLOGY

This section will develop an initial survey structure and ask experts' opinions on the study and the questions. Additionally, the number of survey questions and content will be determined, and the final model applied for the quantitative research will be presented.

3.1. Proposing the Initial Acceptance Model

Based on the discussions carried out in Section 2.9, a high-level adoption model is proposed as follows:

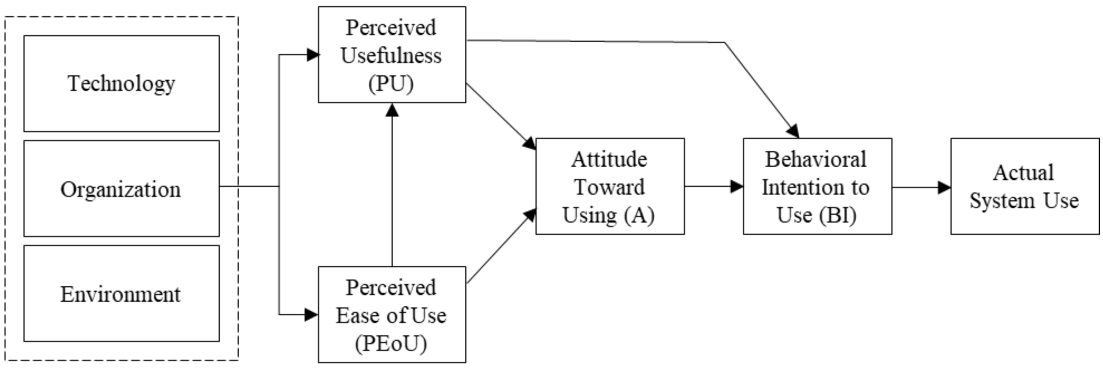


Figure 27 High-level adoption model (TOE integrated with TAM)

All the factors that may affect adoption in the context of technology, organization, and environment on the model can be presented in Figure 28 below:

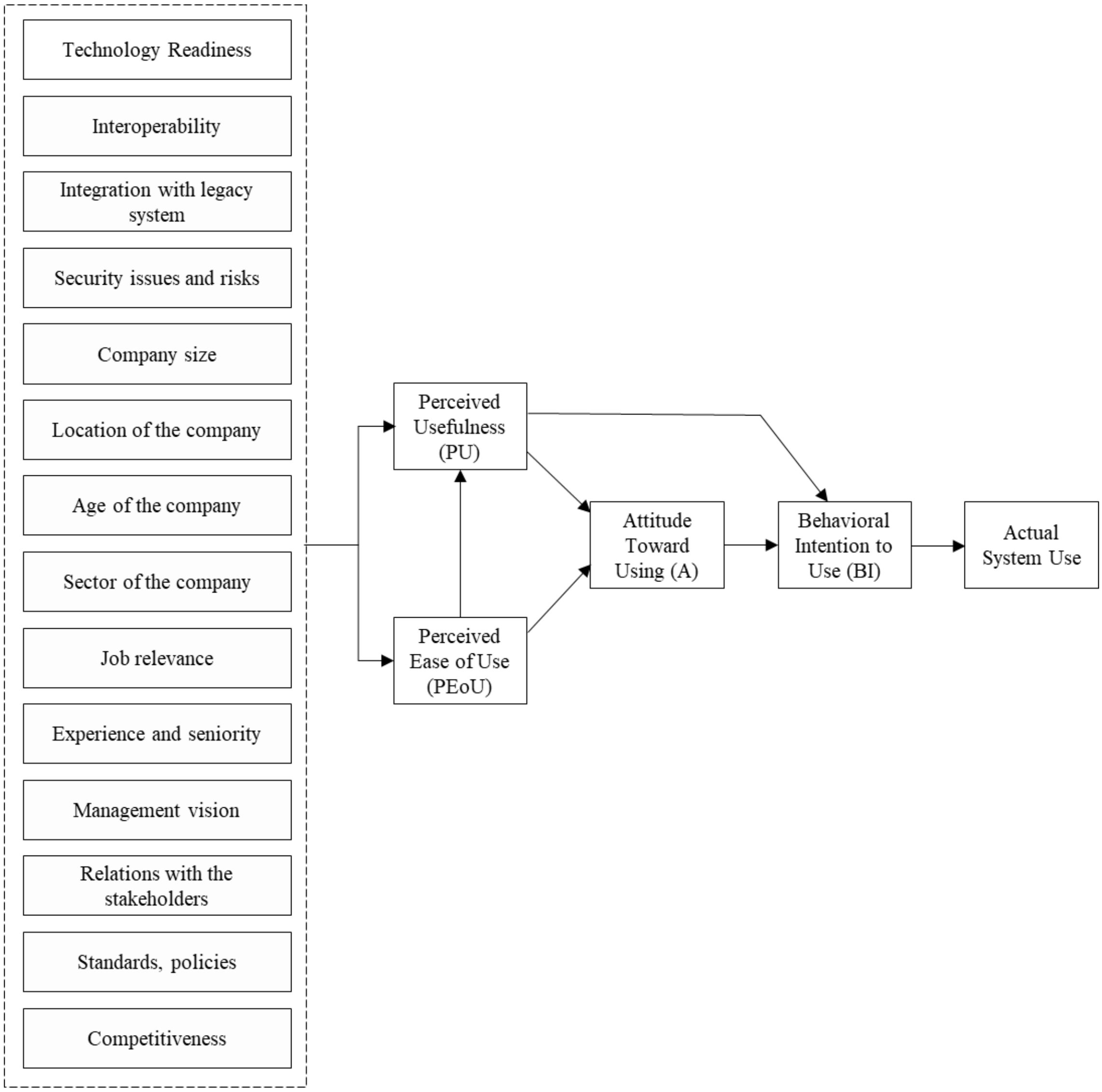


Figure 28 Initially proposed adoption model

3.2. Discussions with the experts

In July 2021, we met with 11 experts working in the sector who have actively used IIoT and are familiar with the technology to get their thoughts on the model we developed and listen to their recommendations. We have listed the positions of these experts and their background with IIoT Technologies in the table below.

Table 16 Information about experts

Expert	Industry	Position	IIoT Experience
[expert 1]	Chemicals	IT Manager	Less than two years
[expert 2]	Plastics and rubber	OT Supervisor	5 years
[expert 3]	Retail	IT Support Manager	5 years
[expert 4]	Glass manufacturing	OT Director (VP)	+10 years
[expert 5]	ICT (vendor)	Managing Director	+10 years
[expert 6]	Chemicals	IT System Engineer	7 years
[expert 7]	Retail	Data Analyst	8 years
[expert 8]	Machinery production	Quality Control Mng.	+15 years
[expert 9]	Steel production	IT Director	10 years
[expert 10]	Food	Operations Manager	None
[expert 11]	Chemicals	Procurement Mng.	2 years

In these meetings, we first tried to understand experts' positive or negative opinions about IIoT and the benefits IIoT provides for them and their companies. Afterward, we received their feedback on the survey structure and possible questions. Except for [expert 6] and [expert 11], we conducted all the interviews face-to-face in Istanbul and completed the discussions within 15 days.

We also interviewed these experts to provide qualitative data to our survey. Here are some ideas we got from the experts:

Table 17 Expert Advice

Experts	Recommendations relevant to the topic *(in short form)*
[expert 1]	To focus on KVKK *(not to ask any personal identification questions).* Everything influences everything *(to keep it as it is).*
[expert 2]	To remind all OT experts once a week. Otherwise, they would not spare any time.
[expert 3]	To focus on trust and privacy *as they are suffering from data leakage.*
[expert 4]:	Organization-related questions do not influence anything—no need to include them.
[expert 5]:	To keep it short and straightforward. ROI expectation influences neither (PU) nor (PEoU), just (BI).
[expert 6]:	Security is the most crucial factor. It influences everything. Besides, trust in partners is another problem.
[expert 7]:	To shorten the survey and focus on security issues. PR directly affects BI.
[expert 8]:	Management support is very much important. C-level must be involved in the project to increase trust and adoption.
[expert 9]:	To focus on interoperability *(as they are in IIoT roll-out project and suffering from integrations and interoperability)*. (CO) may also affect (BI). The survey is too long.
[expert 10]:	35-40 questions would be more than enough. Focus on just problems, not generic.
[expert 11]:	To add industry-specific questions.

After receiving the experts' opinions, we decided to change our entire structure and the number of questions. We reduced the total number of questions from 80 to 50 and Likert scale type questions from 60 to 35.

The final version of the proposed technology acceptance model to be analyzed is presented in Figure 29 below:

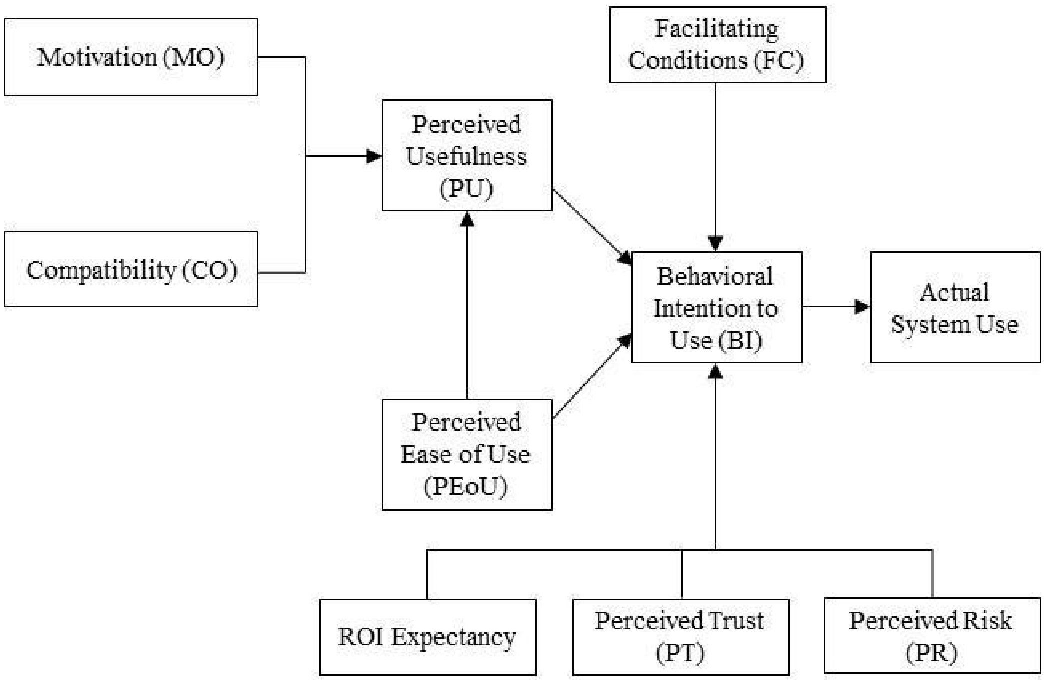


Figure 29 Proposed Technology Acceptance Framework

3.3. Hypothesis Formulation

This section will form our hypotheses and include our survey questions according to the framework study we have created.

3.3.1 Perceived Usefulness

Many previous studies show that the degree of perceived usefulness is directly proportional to the user's intention to use the system. In this case, our following hypothesis is as follows:

> *H1: Perceived usefulness positively affects the behavioral intention of the user to use the IIoT system.*

3.3.2 Perceived Ease of Use

Another factor affecting the user's intention to use IIoT technology is the user's perceived ease of use. In addition, the user's perception of ease of use is directly proportional to the perceived usefulness of that system. In this case, our hypotheses would be as follows:

> *H2: Perceived ease of use affects the behavioral intention of the user to use the IIoT system positively.*

> *H3: Perceived* ease *of use affects the perceived usefulness positively.*

3.3.3 Motivation (MO)

The user's motivation to use a system indicates that the perceived benefit from that system will be higher. Our following hypothesis is as follows:

> *H4: Motivation of the user positively affects perceived usefulness.*

3.3.4 Compatibility (CO)

As mentioned in Section 2.6.1, one of the biggest problems of organizations is the integration and interoperability of IIoT systems with existing systems, so we carried this issue into our study, and we formed our hypothesis as follows:

> *H5: Compatibility positively affects perceived usefulness.*

3.3.5 ROI Expectancy (ROI)

The expectation that there will be a quick return to the systems is an indication that the user intends to use the system directly. Accordingly, our following hypothesis is as follows:

> *H6: Faster ROI expectancy positively affects the behavioral intention of the user to use the IIoT system.*

3.3.6 Perceived Trust (PT)

As we examined in Section 2.6.2, IIoT systems have very complex structures. The fact that the stakeholders do their job correctly and the trust placed in them is vital to a successful project. Our following hypothesis is as follows:

> *H7: Perceived Trust positively affects the behavioral intention of the user to use the IIoT system.*

3.3.7 Perceived Risk (PR)

In Section 2.6.2 and Section 2.6.4, we identified security risks at the top of the challenges experienced in IIoT systems. The greater the perceived threat, as one of the most critical factors, the lower the system's adoption will be. Our hypothesis regarding security is as follows:

> *H8: Perceived Risk negatively affects the behavioral intention of the user to use the IIoT system.*

3.3.8 Facilitating Conditions (FC)

Facilitating conditions are the management's ownership of the project, providing training, and providing convenience to the employee. In this case, the more the management owns the project, the easier it will be to adopt the system. Our hypothesis regarding the facilitating conditions is as follows:

> *H9: Facilitating Conditions positively affect the behavioral intention of the user to use the IIoT system.*

In this case, we have prepared our survey questions as listed below:

Table 18 Survey Questions

Construct	**Questions**
Perceived Usefulness (PU) – *Likert Scale*	
PU 1	I can complete my tasks faster with IIoT products and applications
PU 2	I can be more productive at work thanks to IIoT products and applications
PU 3	Using IIoT products and applications can make my job easier
PU 4	I find IIoT products and applications useful for my business
Perceived Ease of Use (PEoU) – *Likert Scale*	
PEoU 1	I can easily learn to use IIoT products and applications.
PEoU 2	I want to use IIoT products and applications to achieve what I want.
PEoU 3	Using IIoT products and applications does not require much mental and physical effort.
PEoU 4	I would find IIoT products and applications easy to use.
Motivation (MO) – *Likert Scale*	
MO 1	Advances in IIoT technology excite and motivate me.
MO 2	IIoT products and applications are very much applicable to my tasks.
Compatibility (CO) – *Likert Scale*	
CO 1	I think IIoT products and services can easily integrate into existing systems
CO 2	I think IIoT products and services can easily communicate with each other.
CO 3	I think IIoT devices can easily integrate into our company’s IT and OT networks
ROI Expectancy (ROI) – *Likert Scale*	
ROI 1	I think the cost of a possible IIoT project is not an obstacle for our company
ROI 2	I think the benefits of IIoT will overweigh the implementation costs
ROI 3	IIoT technology plays an essential role in reducing operational costs
ROI 4	It is possible to obtain an acceptable ROI from the application of IIoT technology.

Table 18 (cont.)

ROI 5	IIoT Technology would enable my organization to be more competitive and increase my market share.
ROI 6	IIoT Technology would enable my organization to penetrate new markets.
Perceived Trust (PT) – *Likert Scale*	
PT 1	IIoT products and applications are trustworthy
PT 2	I rely on the data I collect from IIoT sensors.
PT 3	In a possible project, IIoT sensors will securely communicate with each other.
PT 4	The outputs of IIoT Products and applications that I use are error-free.
PT 5	IIoT products and application providers will fulfill their commitments in a possible project.
PT 6	I am confident that IIoT technology providers protect me from any problems I may encounter.
Perceived Risk (PR) – *Likert Scale*	
PR 1	Failure of an IIoT device in my network can lead to complicated problems.
PR 2	A possible cyber-attack on the IIoT infrastructure I use may significantly affect my company's operation.
PR 3	The security issues of IIoT technology affect my investment plans in this technology.
PR 4	Organizations that regulate standards need to step up for better communication of interconnected devices.
PR 5	It worries me that IIoT products on my network are constantly connected to the Internet.
Facilitating Conditions (FC) – *Likert Scale*	
FC 1	Our board of directors and senior executives agree that IIoT technology is necessary for our company to thrive.
FC 2	We have sufficient knowledge and staff to deploy and manage an IIoT system.
FC 3	Our company has plans to implement an IIoT project in the next two years.
Behavioral Intention (BI) – *Likert Scale*	
BI 1	I see IIoT technologies as a benefit to our organization.
BI 2	I want to use IIoT products and applications on my network given a chance.

3.4. Data Analysis Method

The data analysis presents descriptive statistics as frequency, percentage, mean, and standard deviation in determining the reliability level of the Likert-type scales used in the study, Co. Alpha test and factor analysis were performed. A repeated ANOVA test examined the difference between the obtained technology sub-dimensions. Independent sample t-test and ANOVA test were conducted to explore the differences in the sub-dimensions of the technology acceptance model in the study considering the characteristics of the participants and their companies. Correlation analysis was performed to examine the relationship between the technology acceptance model sub-dimensions and organizational and technological readiness. Analyzes were made with SPSS 21.0 package program.

CHAPTER 4

SURVEY ANALYSIS AND FINDINGS

In this section, we will explain our survey structure, strategy and interpret the results we obtained:

4.1. Survey Structure

Our survey aimed to determine the ease of use, usefulness, challenges, and risks of IIoT technology, which has become widespread with significant momentum in businesses in recent years.

In this case, a criteria sampling strategy (Patton, 2015) was applied to target participants with specific knowledge experience on the subject (Moser & Korstjens, 2021). The target audience were experts from different sectors and regions who were experienced in using industrial control systems or Industry 4.0 applications and closely followed developments in this field. In addition to the primary audience, we also aimed to reach experts working in IT, marketing, data collection, and business analysis, working in less risky departments with the potential to use IIoT technology.

Upon the advice of the experts we interviewed, we decided not to limit our survey to only Turkey. In this way, we aimed to measure the perspectives of different cultural structures on IIoT technology. Within the scope of the research, we targeted to reach participants from different sectors, including energy, mining, technology, health, retail, and many other industries, so that we have a chance to analyze the perspectives and competencies of experts with the same position in different sectors on IIoT technology.

We completed our study in two phases as qualitative and quantitative research. We will present the results of these investigations in the following sections.

4.2. Qualitative Analysis

As part of our research, we interviewed 11 experts in July 2021. These experts were active users of IIoT technology, and most of their work was built on IIoT technology. We tried to meet experts from different sectors and in different positions. Our targets from these meetings were as follows:

- To get their opinions on the survey (which we will use for quantitative data analyzes)
- To determine what they are using IIoT for
- Learn the core values that IIoT technology brings to them
- Learning about the difficulties they experience while using technology
- Get their thoughts on the future of IIoT technology

Open-ended questions were prepared for participants with a certain experience level on the subject, considering the phenomenological approach (Flick, 2018). This approximation method aimed to analyze participants' experiences with IIoT technology in detail (Vagle, 2018). We paid attention that the answers given by the participants were not in a specific structure. The first two questions were chosen so that the participant could answer without difficulty (Mathers, 2021). In the interviews, we also paid particular attention not to reflecting our comments and thoughts on the subject and not receiving any personal information from the participants (Liedtka, 1992). To make an accurate analysis, we stated before the interviews that the answers from the participants should have been between 40 and 50 words and that the answers should have included the keywords about IIoT technology (Züll, 2021):

In this context, the following questions were asked to the industry professionals:

1) What does IIoT mean to you?
2) How close do you see IIoT technology to yourself and your business?
3) What are the obstacles of IIoT to the widespread use in critical infrastructures and production lines?
4) What do you think about the possible problems in the convergence of IT and OT structures?
5) What are your expectations from IIoT technology within the scope of Industry 4.0 applications?
6) What are your expectations for IIoT technology to adapt to your current IT/OT environment?

From Section 3.2, the list of experts we interviewed was as follows:

Expert	Industry	Position	IIoT Experience
[expert 1]	Chemicals	IT Manager	Less than two years
[expert 2]	Plastics and rubber	OT Supervisor	5 years
[expert 3]	Retail	IT Support Manager	5 years
[expert 4]	Glass manufacturing	OT Director (VP)	+10 years
[expert 5]	ICT (vendor)	Managing Director	+10 years
[expert 6]	Chemicals	IT System Engineer	7 years
[expert 7]	Retail	Data Analyst	8 years
[expert 8]	Machinery production	Quality Control Mng.	+15 years
[expert 9]	Steel production	IT Director	10 years
[expert 10]	Food	Operations Manager	None
[expert 11]	Chemicals	Procurement Mng.	2 years

We presented the experts' recommendations regarding our survey in the previous section. The essential parts of their views on the topics listed above are as follows.

Table 19 Experts' expectations and their opinions on core values and challenges of IIoT

Expert	**Usage**	**Core values**	**Challenges**	**Expectations**
[expert 1]	Quality control purposes	Automated monitoring and control	Sensor failures due to environmental conditions	Improvement on the sensor side
[expert 2]	Data collection from the machines	Predicting maintenance periods and analyzing machine performances	Sensor interoperability. They have cases where two sensors from different companies but cannot communicate for the same purposes.	Standardization in communication and sensor types
[expert 3]	Data collection from their retail stores. >more than 3000 sensors.	Customer analytics. They understand their customers' shopping behaviors by analyzing people, demographics, and queue abandonment rates.	They have recently been faced with the data flow. The supplier mistakenly shared all customers' performances with all stores activating in the same field. They decided to change their suppliers.	She expects a more robust and secure system that eliminates the need for the cloud.
[expert 4]	Everything about the production: the company has 16 factories in 6 countries worldwide, and they are all connected.	Factory performance measurement.	They suffer from 3rd party presence of their suppliers inside the factory. Besides, AI-based systems are not accurate.	Improvements on the AI side.
[expert 5]	He is the representative of a global company in Turkey. They provide their IIoT platform to the manufacturing companies in Turkey.	He believes that IIoT technology increases the competitiveness of the companies.	Affordability. All the prices are in USD, and due to fluctuation in TRY, the companies face difficulties in supplying their systems and spare parts. They also suffer from integration works with ICS infrastructure.	He expects reductions in prices, which can be possible with more companies adopting the technology.

[expert 6]	Remote monitoring the machine park	Thanks to data analysis, they predict the increase or decrease in production and monitor everything inside the factories in real-time.	Security. They had an attack two months ago, and they think it happened because of the vulnerabilities in the gateways connected to the cloud.	They expect a more secure structure allowing on-prem installations.
[expert 7]	He analyzes the data from their >500 stores located in 18 different countries.	Thanks to IIoT technology, they make better decisions on opening new stores, shutting down the underperforming ones. They also plan and develop all their marketing activities based on the analyses.	Accuracy of the sensors. The vendor guarantees 99% accuracy, but they have never seen above 80%s.	They expect more accurate sensors and improvements in the cloud.
[expert 8]	They produce IIoT sensor embedded machines, which are used for production.	They can remotely analyze their machines in the field and plan and provide maintenance services accordingly.	They suffer from very few qualified resources who understand the IIoT business. Besides, they face problems integrating their new generation machines into existing infrastructures without IIoT.	He expects more qualified people and ease of integration with the existing machines.
[expert 9]	They collect data from their boilers to adjust the heat of the environment.	Remote controlling and employee safety. After IIoT, they do not need to come close with the boilers and other dangerous equipment.	They suffer from inadequate business partners and the vel of technical support. They are based in Karabük, and almost every day, they open more than 5 critical tickets to the supplier.	IIoT is used to measure the machines' performances in the field, but they lag in predicting their performances. With the combination of digital twin and AI technologies, they are expecting new changes in the technology very soon.
[expert 10]	She is not actively using the technology, but they use the system for quality control purposes as a company.	The most important value is to enable humanless quality control, thereby more hygiene.	They suffer from their applications and high recurring fees to their suppliers.	They expect more user-friendly applications and reduced recurring fees.

[expert 11]	They use more than 1000 sensors in their factories located in Gebze and Gaziantep as a company. They collect the data from the machines to analyze their performances.	With IIoT, they can coordinate shifts, adjust energy consumptions.	They suffer from long lead periods. They have to wait for 5 to 6 weeks to supply their sensors. They also have problems with integrations.	Shorter lead times. More flexible sensors.

4.2.1. Results of Qualitative Analysis

As a significant result of qualitative research, the experts predominantly use IIoT technology primarily for data analysis. Besides, the most critical expectation from IIoT technology is to make quicker and more accurate decisions thanks to remote monitoring and control capabilities. The difficulties they faced in using IIoT technology were very different from each other, which can be listed as the reliability problems of the sensors, the security of their infrastructure, and privacy concerns due to their dependence on the cloud system.

Despite these problems, we observed that security measures remained in the background. We interpreted this situation as the benefit obtained from the systems outweighing the risks. Suggestions on this topic will be given in the conclusion section.

4.3. Quantitative Analysis

The quantitative research was conducted in August and September 2021. As mentioned before, our research criteria were as follows:

- Experts working in various sectors who actively use or tend to use IIoT technology
- *Preferably*, employees with technical backgrounds who personally experience existing problems, if any

We aimed to reach 1000 people at the beginning of the research period in this context. We could have accessed 527 people and submitted our survey prepared in English and Turkish on the METU Survey platform. In return, we received answers from 342 people. Accordingly, our success rate is around 65%.

The research was carried out entirely online. The most crucial issue that we had difficulty with within the scope of our research study was the structure of the questionnaire. We prepared 80 questionnaires by synthesizing the literature review's questions about technology acceptance models. However, after the experts' feedback, we removed more than half of these questions. The biggest reason for this was that the companies were too busy to meet the demands after the COVID measures and therefore could not spare time.

Our goal was to conduct this research in February and March 2021, but we realized that many factories work part-time due to lockdowns. Due to lack of time, we could not conduct a pilot study.

4.3.1. Survey Findings

The full statistical breakdown of our survey can be found in Appendix C. In the survey, questions such as age, name, age, which contain personal information, were not asked upon the advice we received from the experts. The region where the head office is located, the number of employees, the use of technology, IIoT history, the position, and the respondent's department were asked. They were also asked about the 3 most essential benefits that IIoT technology brings to them and the 3 biggest challenges they face. Here we will summarize all our findings.

Three hundred forty-two people participated in our survey. Among 342 people, 255 people attended from Turkey and 87 people abroad. The highest participation abroad was from the European region with 29 people. Europe is followed by the Middle East and Africa region with 27 people and Asia with 22 people. Perhaps the most striking result of the survey is the participation from more than 30 different sectors. The first five sectors are food with 30 people, the chemical industry with 25 people, plastic and rubber with 23 people, iron and steel production with 21 people, and paper and packaging industry with 19 people.

60% of the experts work in organizations operating for 10 years or more. Again, more than 60% are organizations with between 100 and 2000 employees. The number of organizations with 5000 or more employees is 45.

There are both IT and OT functions where 208 people work. This situation was interpreted as most manufacturing companies responded to the survey. The organization with 296 employees has a particular digital transformation strategy. Finally, the organization employing 288 people currently uses IIoT technology. This number is 84%. As such, it is in line with the 86% rate found in Microsoft's IoT Signal survey conducted across Europe in October 2021 (Microsoft & Hypothesis, 2021). In the company where 188 people work, there are both IT and OT functions, Digital Transformation Strategy, and IIoT usage.

One hundred sixty of the respondents are in the IT department, and 88 are in the OT department. Fifty-three of the participants work in the engineering department. In other words, nearly 90% of the respondents are of technical background. About 250 people out of 342 are mid-level managers in their organizations.

To our question about Industry 4.0 technology, which will become the most widespread in the next 5 years, with a single-choice answer, 127 participants said IIoT. One hundred fifteen people said artificial intelligence. In this respect, artificial intelligence-based IIoTs, which we discussed in Section 2.4.1, are of great importance. The background of 150 respondents with IIoT varies between 3 and 5 years. The number of people with less than 3 years and more than 5 years of experience is also balanced. In this respect, we can say that the average IIoT expertise of the participants is between 3-5 years.

To the question that we asked about the most significant benefits of IIoT with three options, 155 people said automated equipment management, 127 people said eliminated human errors, 121 people said better and faster production, and 113 people said better asset management. When we analyze the results on a sectoral basis, a completely different picture emerges. For example, while the most crucial benefit for the food industry is increased product quality and rapid production, the most critical issue for the mining industry is human safety. For the telecommunications industry, remote management capability is far ahead.

Finally, 189 people complained of interoperability and integration problems. We also experienced this situation with the experts we interviewed one-on-one. One hundred seventy-seven people complain about the inadequacy of the partners. Interestingly, the rate of those who complained about security remained at 164. We can explain this reason as the importance of security emerges in case of vulnerability or any threat. Likewise, when we analyze on a sector basis, we see that the biggest challenge for the food sector is interoperability. At the same time, the shortage of qualified employees and costs come to the fore for the mining sector. For the telecommunications industry, interoperability and security are at the forefront.

After this section, our analysis of the applied acceptance model will be given. The analyzes were made on SPSS 21.0, and the reports are included in Appendix D with their integrity intact.

4.3.2. Reliability Analysis

Researchers have recognized Cronbach's alpha (Cronbach, 1951) value as one of the most important measurements used to demonstrate the reliability of research (Bonett & Wright, 2014). Values between 0 and 1 and results close to 1 mean more reliable. Cronbach's alpha value should be above 0.7 for general and each construct (Gliem & Gliem, 2003).

Accordingly, the Cronbach's alpha value of our study is as follows:

Table 20 Overall Cronbach’s alpha analysis *(retrieved from SPSS 21)*

Overall Cases	N	%	**Cronbach’s Alpha**	**N of items**
Valid	342	100	0,942	35
Excluded	0	0		
Total	342	100		

Table 21 Cronbach’s alpha analysis per construct *(retrieved from SPSS 21)*

Other Constructs	**Cronbach’s Alpha**	**N of items (∑ = 35)**
Perceived Usefulness (PU)	0,926	4
Perceived Ease of Use (PEoU)	0,894	4
Motivation (MO)	0,826	2
Compatibility (CO)	0,861	3
ROI Expectancy (ROI)	0,905	6
Perceived Trust (PT)	0,953	6
Perceived Risk (PR)	0,811	5
Facilitating Conditions (FC)	0,776	3
Behavioral Intention (BI)	0,893	2

The tables above show that Cronbach's alpha value falls into the excellent grade. While we observed relatively low values for some of the other factors, we decided not to do anything for now, as they were all greater than the lowest acceptable value of 0,7.

4.3.3. KMO and Anti-image Correlation Analysis

The Kaiser-Meyer-Olkin (KMO) test measures how well data is suitable for Factor Analysis. The test measures sampling adequacy for each variable and the entire model. KMO returns values between 0 and 1 (Opitz et al., 2012; Field, 2009). A basic rule of thumb for interpreting statistics:

- KMO values between 0.8 and 1 indicate adequate sampling.
- KMO values less than 0.6 indicate that sample is not sufficient and corrective action should be taken.
- KMO Values close to zero mean there are significant partial correlations compared to the sum of the correlations. In other words, there are common correlations that are a big problem for factor analysis.

In our case, the KMO value is as follows:

Table 22 KMO value analysis *(retrieved from SPSS 21)*

Kaiser – Meyer – Olkin (KMO) Measure of Sampling Adequacy	**0,92**
Approx. Chi-Square	10411,807
df	595
Sig	.000

The above table shows that the KMO value is 0.92, and Bartlett's test significance value is 0.000 (which should be a value below 0,05). These results reveal that our research is ideal for evaluation (Toni et al., 2021).

The anti-image correlation matrix contains the negatives of the partial correlation coefficients, and the anti-image covariance matrix has the negatives of the partial covariances. In a good factor model, most of the off-diagonal elements of anti-image matrices should be over 0,5. The measure of sampling adequacy for a variable is displayed on the diagonal of the anti-image correlation matrix (Castle et al., 2011).

Table 23 AIC – MSA value analysis for each question *(retrieved from SPSS 21)*

Item	**AIC – MSA value**
PU1	0,924[a]
PU2	0,909[a]
PU3	0,939[a]
PU4	0,938[a]
PEoU1	0,904[a]
PEoU2	0,935[a]
PEoU3	0,858[a]
PEoU4	0,865[a]
MO1	0,958[a]
MO2	0,948[a]
CO1	0,959[a]
CO2	0,914[a]
CO3	0,919[a]

Item	**AIC – MSA value**
ROI6	0,896[a]
PT1	0,958[a]
PT2	0,936[a]
PT3	0,950[a]
PT4	0,950[a]
PT5	0,917[a]
PT6	0,942[a]
PR1	0,717[a]
PR2	0,723[a]
PR3	0,805[a]
PR4	0,825[a]
PR5	0,799[a]
FC1	0,902[a]

Table 23 (Cont.)

ROI1	0,945[a]	FC2	0,947[a]
ROI2	0,947[a]	FC3	0,961[a]
ROI3	0,917[a]	BI1	0,892[a]
ROI4	0,928[a]	BI2	0,884[a]
ROI5	0,898[a]		

Since none of the above values are below 0.5, we continue our analysis with the rotated factor matrix. We selected "Maximum Likelihood" as the extraction method to calculate Rotated Factor Matrix and "Varimax" as the rotation method. As we have 9 different factors, we entered the value 9 as the maximum iterations for convergence. From the options menu, we set the minimum value 0,4. The analysis has returned the below results:

Table 24 Rotated Factor Matrix Analysis *(retrieved from SPSS 21)*

	Rotated Factor Matrix						
	Factor						
	1	2	3	4	5	6	7
PT4	0,896						
PT5	0,889						
PT3	0,845						
PT6	0,822						
PT2	0,744						
PT1	0,710						
CO3	0,568						
CO2	0,542						
CO1	0,505						
PEoU3		0,906					
PEoU4		0,890					
PEoU2		0,670					
PEoU1		0,603					
MO1		0,533					
MO2		0,425					
ROI3			0,792				
ROI2			0,762				
ROI4			0,711				
ROI1			0,518				
PU2				0,824			
PU1				0,777			
PU3				0,755			
PU4				0,587			
BI1					0,812		
BI2					0,758		
FC3					0,501		
FC1					0,454		
FC2						**N/A**	
PR2						0,903	
PR1						0,740	
PR5						0,636	
PR4						0,575	
PR3						0,524	
ROI6							0,765
ROI5							0,674

We identified exciting findings in this table. First of all, the FC2 value remained below 0.4. On the other hand, our factor number, which was 9 at the beginning, has decreased to 7. Compliance and perceived trust remained in the same group. We named this column (PT) to follow up later in the analysis. Motivation-related items were grouped with PEoU (we called this group PEoU). We noticed the most significant issue was that the 6-item ROI factor was split. We saw that the first 4 items we looked at the questions were really about the costs, while the last two were about the return on investment. Therefore, we created a Cost Efficiency (CE) group, including ROI1, ROI2, ROI3, and ROI4. FC1 and FC3 items were added to the BI group.

4.3.4. Convergent Validity

As a subset of construct validity, convergent validity indicates the strong relationship between the elements of a construct. According to Hair (2009), all factor loadings should be above 0.6 to ensure convergent validity. Besides, composite reliability values should be greater than 0.7, and AVE values for each factor should be greater than 0.5 (Hair, 2009; Huang et al., 2013). To find loadings, CR, and AVE values and, most importantly, to obtain our final path analysis, we used SmartPLS 3.0. First, we can start with the Initial Factor Loadings of the items.

Table 25 Initial Convergent Validity Analysis *(retrieved from SMART PLS 3.0)*

	Cost Efficiency	Intention to Use	Perceived Ease of Use	Perceived Risk	Perceived Trust	Perceived Usefulness	ROI Expectancy
BI1		0.896					
BI2		0.863					
CO1					0.756		
CO2					0.763		
CO3					0.757		
FC1		0.760					
FC3		0.805					
MO1			0.815				
MO2			0.772				
PEoU1			0.714				
PEoU2			0.828				
PEoU3			0.844				
PEoU4			0.843				
PR1				0.757			
PR2				0.884			
PR3				0.451			
PR4				0.678			
PR5				0.829			
PT1					0.855		
PT2					0.863		

Table 25 (Cont.)

PT3					**0.893**		
PT4					**0.879**		
PT5					**0.874**		
PT6					**0.845**		
PU2						**0.926**	
PU3						**0.923**	
PU4						**0.858**	
ROI1	**0.715**						
ROI2	**0.917**						
ROI3	**0.925**						
ROI4	**0.899**						
ROI5							**0.972**
ROI6							**0.970**
PU1						**0.909**	

The table above indicates that we are very close to the end. Only PR3 remained below the threshold value of 0.6. We decided to keep PR4 as it remains above the threshold value. After removing PR3, we recalculated the PLS algorithm and received the following factor loadings table.

Table 26 Initial Convergent Validity Analysis after removing PR3 (retrieved from SMART PLS 3.0)

	Cost Efficiency	**Intention to Use**	**Perceived Ease of Use**	**Perceived Risk**	**Perceived Trust**	**Perceived Usefulness**	**ROI Expectancy**
BI1		**0.896**					
BI2		**0.864**					
CO1					**0.756**		
CO2					**0.763**		
CO3					**0.757**		
FC1		**0.760**					
FC3		**0.805**					
MO1			**0.815**				
MO2			**0.772**				
PEoU1			**0.714**				
PEoU2			**0.828**				
PEoU3			**0.844**				
PEoU4			**0.843**				
PR1				**0.755**			
PR2				**0.886**			
PR4				**0.681**			
PR5				**0.831**			
PT1					**0.855**		
PT2					**0.863**		
PT3					**0.893**		
PT4					**0.879**		

Table 26 (Cont.)

PT5					0.874		
PT6					0.845		
PU1						0.909	
PU2						0.926	
PU3						0.923	
PU4						0.858	
ROI1	0.715						
ROI2	0.917						
ROI3	0.925						
ROI4	0.899						
ROI5							0.972
ROI6							0.970

As we practiced at the very beginning, we again tested Cronbach's Alpha and Composite Reliability and retrieved the following results:

Table 27 Initial Cronbach's alpha, composite reliability, and AVE analysis after grouping (retrieved from SMART PLS 3.0)

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cost Efficiency	0.888	0.904	0.924	0.754
Intention to Use	0.851	0.858	0.900	0.694
Perceived Ease of Use	0.891	0.902	0.916	0.646
Perceived Risk	0.805	0.860	0.870	0.627
Perceived Trust	0.944	0.949	0.953	0.694
Perceived Usefulness	0.926	0.926	0.947	0.818
ROI Expectancy	0.939	0.940	0.971	0.943

Finally, we have reached all green. We see that all values are much higher than their threshold values. As the next step, we will look at discriminant validity.

4.3.5. Discriminant Validity

As the second subset of construct validity, discriminant validity is used to demonstrate the constructs measures, which theoretically should not be highly correlated are not highly correlated. However, in practice, the discriminant validity coefficients should be significantly smaller than the convergent validity coefficients (Cronbach & Meehl, 1955). Below, we present our discriminant validity table:

Table 28 Initial Discriminant Validity Analysis (retrieved from SMART PLS 3.0)

	Cost Efficiency	Intention to Use	Perceived Ease of Use	Perceived Risk	Perceived Trust	Perceived Usefulness	ROI Expectancy
Cost Efficiency	**0.868**						
Intention to Use	0.556	**0.833**					
Perceived Ease of Use	0.486	0.533	**0.804**				
Perceived Risk	-0.107	-0.238	-0.106	**0.792**			
Perceived Trust	0.634	0.550	0.508	0.046	**0.833**		
Perceived Usefulness	0.484	0.591	0.650	-0.020	0.554	**0.905**	
ROI Expectancy	0.717	0.508	0.420	-0.055	0.587	0.475	**0.971**

4.4. Structural Model

Finally, we run the model on SmartPLS and get the below Figure 30:

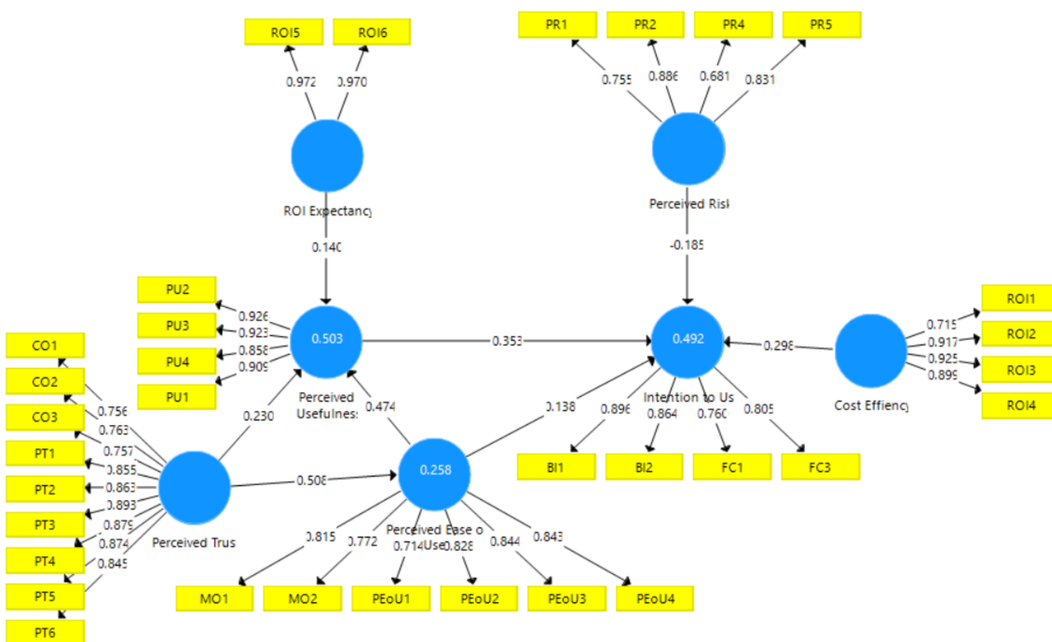


Figure 30 Initial Structural Model Analysis *(retrieved from SMART PLS 3.0)*

Thus, we have obtained our model. Values show that the relevant factor has a positive or negative relationship with the construct to which the arrow is attached. For example, as the degree of perceived usefulness increases, the tendency to use technology also increases. On the other hand, as risk perception increases, the tendency to use technology decreases. Besides, our R square value is 49,2% for this study.

4.5. Analysis of the Final Model

So far, everything looks fine except the R square value, which is 49,2%. We learned from the literature that this value could increase by providing more connection points between factors, so we dived deep into the SmartPLS app again.

For the final model, we removed PR3 and PR4, which were slightly below 0.7 in Outer Loadings in the previous calculation. Considering that the ROI expectation may also affect the PEoU and the PT may also affect the BI, we made the necessary connections. In this model, we also evaluated FC2, which was below 0.4 in Rotated Matrix Analysis in SPSS.

After making all the connections, we got the following model for factor analysis:

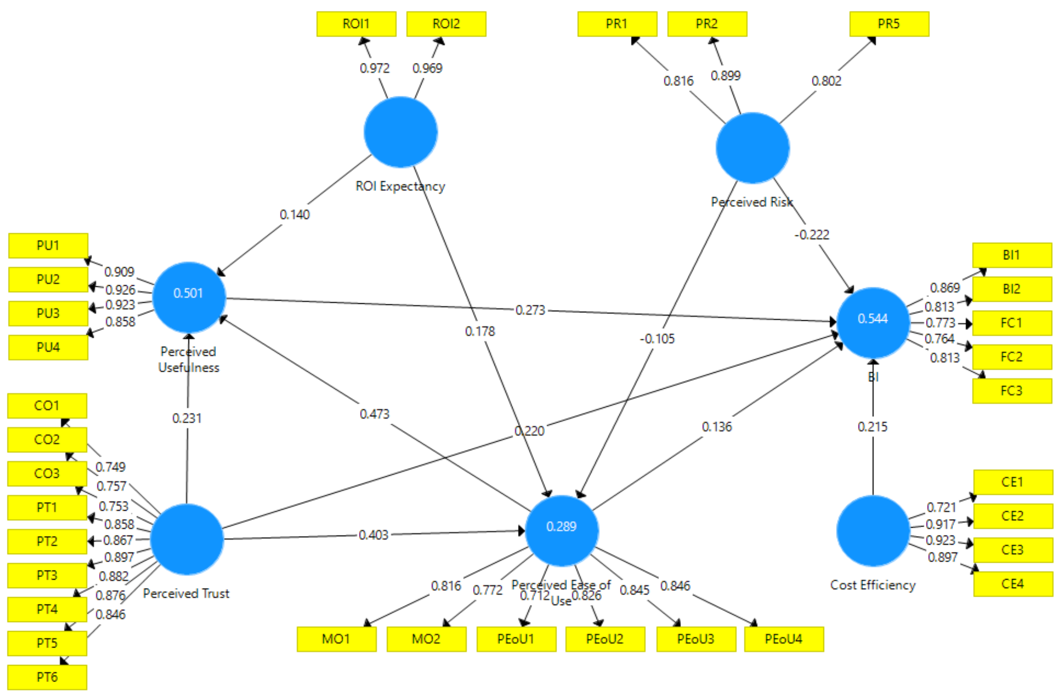


Figure 31 Factor analysis of the Final Model *(retrieved from SMART PLS 3.0)*

We found that the effect of the PT factor on BI, PU, and PEoU was significant in this model. We also found that the R squared value is 54.6%, and the adjusted R squared value is 53.9%. According to Chin, studies with an R square value above 0.67 are valuable. Values between 0.67 and 0.33 are moderately valuable (Chin, 1998). On the other hand, the average R square value of Acceptance models made on IoT in the literature is around 0.5. In this respect, we can say that our study has a degree above the average.

In addition to factor analysis, we can also quickly obtain path analysis and Beta values with SmartPLS 3.0. According to Kock, the higher the Beta value, the more effective it is (Kock, 2016). The model of our beta and roadmap is as shown in Figure 32 below:

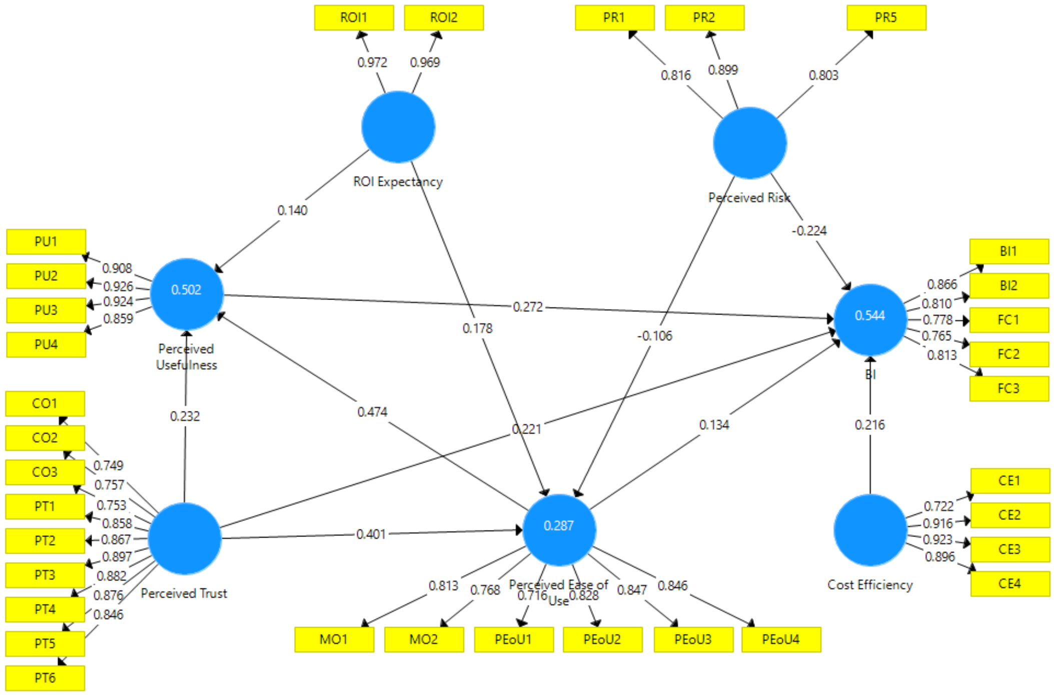


Figure 32 Beta (β) and Path Analysis of the Final Model

To give an example from the values above, for example, the positive effect of PT on BI is 22.21%. On the other hand, PR has a negative impact with 22.4% on BI.

4.5.1. Convergent validity analysis of the final model

For the factors to be valid, each factor load must be greater than 0.7 (Ahmed et al., 2020; Sarstedt, Ringle & Hair 2017). Next, we will look at our "Outer Loadings" values and obtain Table 29 below:

Table 29 Final Convergent Validity Analysis (retrieved from SMART PLS 3.0)

	BI_	**Cost Efficiency**	**Perceived Ease of Use**	**Perceived Risk**	**Perceived Trust**	**Perceived Usefulness**	**ROI Expectancy**
BI1	**0.869**						
BI2	**0.813**						
CE1		**0.721**					
CE2		**0.917**					
CE3		**0.923**					
CE4		**0.897**					
CO1					**0.749**		
CO2					**0.757**		
CO3					**0.753**		
FC1	**0.773**						
FC2	**0.764**						

Table 29 (Cont.)

FC3	0.813						
MO1			0.816				
MO2			0.772				
PEoU1			0.712				
PEoU2			0.826				
PEoU3			0.845				
PEoU4			0.846				
PR1				0.816			
PR2				0.899			
PR5				0.802			
PT1					0.858		
PT2					0.867		
PT3					0.897		
PT4					0.882		
PT5					0.876		
PT6					0.846		
PU1						0.909	
PU2						0.926	
PU3						0.923	
PU4						0.858	
ROI1							0.972
ROI2							0.969

In our table, factor values vary between 0.712 and 0.972. Since there is no value less than 0.7, we can say that our factor loads are valid and reliable.

4.5.2. Reliability analysis of the final model

Next, we will evaluate Cronbach's Alpha, Composite Reliability, and AVE evaluation values for each factor. This assessment is shown in Table 30 below:

Table 30 Final Cronbach’s alpha, composite reliability, and AVE analysis after grouping *(retrieved from SMART PLS 3.0)*

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
BI_	0.866	0.868	0.903	0.651
Cost Efficiency	0.888	0.9	0.924	0.754
Perceived Ease of Use	0.891	0.902	0.916	0.647
Perceived Risk	0.791	0.793	0.878	0.706
Perceived Trust	0.944	0.948	0.953	0.695
Perceived Usefulness	0.926	0.926	0.947	0.818
ROI Expectancy	0.939	0.941	0.971	0.943

While Cronbach's alpha value evaluates the relationship between factors, Composite reliability evaluates the total performance of the elements on the scale. In other words, Cronbach's alpha measures the factors vertically, while Composite Reliability (CR) measures the scale horizontally (Fornell & Larcker, 1981; Brunner & Süβ, 2005). On the other hand, AVE investigates whether the items that make up the factors are sufficient for the measurement (Thompson, Higgins & Howell, 1994). For example, in our research, the AVE value for PU is 0.818. This value means that 81.8% of the variations in perceived usefulness can be measured with the four questions that make up the PU factor.

For the research to be considered safe, the Cronbach's alpha value should be greater than 0.7 (Nunnally & Bernstein, 1994). In addition, the CR value should also be more significant than 0.7 (Hair, 2009). Finally, the AVE value should be greater than 0.5 (Thompson, Higgins & Howell, 1994).

In our table, we see that these values are easily met. Therefore, we can say with certainty that our research is reliable.

4.5.3. Discriminant validity analysis of the final model

The next step will be Discriminant Validity Analysis, as stated in Table 31 below:

Table 31 Final Discriminant Validity Analysis *(retrieved from SMART PLS 3.0)*

	BI_	Cost Efficiency	Perceived Ease of Use	Perceived Risk	Perceived Trust	Perceived Usefulness	ROI Expectancy
BI_	**0.807**						
Cost Efficiency	0.575	**0.868**					
Perceived Ease of Use	0.552	0.486	**0.804**				
Perceived Risk	-0.26	-0.101	-0.104	**0.84**			
Perceived Trust	0.57	0.634	0.505	0.025	**0.834**		
Perceived Usefulness	0.593	0.483	0.649	-0.031	0.552	**0.905**	
ROI Expectancy	0.516	0.716	0.421	-0.052	0.588	0.475	**0.971**

Discriminant validity tests whether concepts or measures that should be related are genuinely irrelevant (Streiner et al., 2015). In this case, the values placed in the diagonal of the above table must be different and more prominent than the values below. The more diverse these values are, the more difference between the measured factors (Linda et al., 2014). As a result, the values in our table are in line with the literature; therefore, we can say that our factors are successful in measuring the different characteristics of the respondents.

4.5.4. Model Fit

One of the most important ways to understand whether our study is applicable or not is to measure the SRMR - Standardized Root Mean Square Residual and p values. The SRMR value of our study was 0.077. According to Kenny, 2020, this value should be below 0.08 (Kenny, 2020; Hu & Bentler, 1999). Values below 0.08 are considered a "good fit." According to Kenny, the SRMR value increases as the number of samples decreases. In other words, the number of samples is sufficient for values below 0.08. In this respect, we can say that our research is applicable (Mital et al., 2017; Kenny, 2020).

We can look at T statistics and P values to examine whether our model fits factor-wise and ultimately measure whether our hypotheses are supported. The T-value explains the differences within a group. The higher this value, the more different the groupings are and the more valuable it is for statistically determining the overall trend. According to the literature, this value is expected to be greater than 1.8 (Morienyane & Marnewick, 2019; Al-Momani et al., 2018; Yang et al., 2021).

Another value measured together with the T value is the P-value. This value ranges from 0% to 100%, and the closer it is to zero, the more valuable it is. The 0% can be explained so that the outcome is not necessarily due to chance (Salloum et al., 2019; Man et al., 2020; Isaac et al., 2016; Boer et al., 2018). For example, a P-value of 0.03 indicates that the relevant factor may depend on up to 3% chance. To measure these values and evaluate our hypotheses, we can perform bootstrapping with 5000 subsamples on SmartPLS 3.0. The results of bootstrapping are shown in Table 32 below:

Table 32 Bootstrapping of the final model with 5000 subsamples and evaluation of hypotheses *(retrieved from SMART PLS 3.0)*

	Original Sample (O)	**Sample Mean (M)**	**Standard Deviation (STDEV)**	**T Statistics (|O/STDEV|)**	**P Values**	**Hypothesis test**
Cost Efficiency -> BI_	0.215	0.217	0.065	3.337	0.001***	**Supported**
Perceived Ease of Use -> BI_	0.136	0.139	0.06	2.275	0.023**	**Supported**
Perceived Ease of Use -> Perceived Usefulness	0.473	0.475	0.052	9.034	0***	**Supported**
Perceived Risk -> BI_	-0.222	-0.225	0.049	4.496	0***	**Supported**
Perceived Risk -> Perceived Ease of Use	-0.105	-0.107	0.053	1.995	0.046**	**Supported**
Perceived Trust -> BI_	0.22	0.218	0.062	3.568	0***	**Supported**
Perceived Trust -> Perceived Ease of Use	0.403	0.401	0.061	6.649	0***	**Supported**
Perceived Trust -> Perceived Usefulness	0.231	0.23	0.061	3.804	0***	**Supported**
Perceived Usefulness -> BI_	0.273	0.264	0.067	4.092	0***	**Supported**
ROI Expectancy -> Perceived Ease of Use	0.178	0.178	0.064	2.792	0.005***	**Supported**
ROI Expectancy -> Perceived Usefulness	0.14	0.138	0.06	2.353	0.019**	**Supported**

*p<0,1 - **p<0,05 - ***p<0,01

As seen from the table above, our p values are strong. In addition, we can detect unsupported factors with the same method:

Table 33 Not Supported hypotheses *(retrieved from SMART PLS 3.0)*

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Hypothesis test
Cost Efficiency -> Perceived Usefulness	0.022	0.031	0.085	0.265	**0.791**	**Not supported**
ROI Expectancy -> BI_	0.076	0.07	0.059	1.283	**0.2**	**Not supported**
Perceived Risk -> Perceived Usefulness	0.03	0.03	0.055	0.553	**0.58**	**Not supported**

4.5.5. *Theoretical Framework*

After all these analyzes we have made, we can propose our theoretical framework that can be used to measure the adoption of IIoT technology as in Figure 33below:

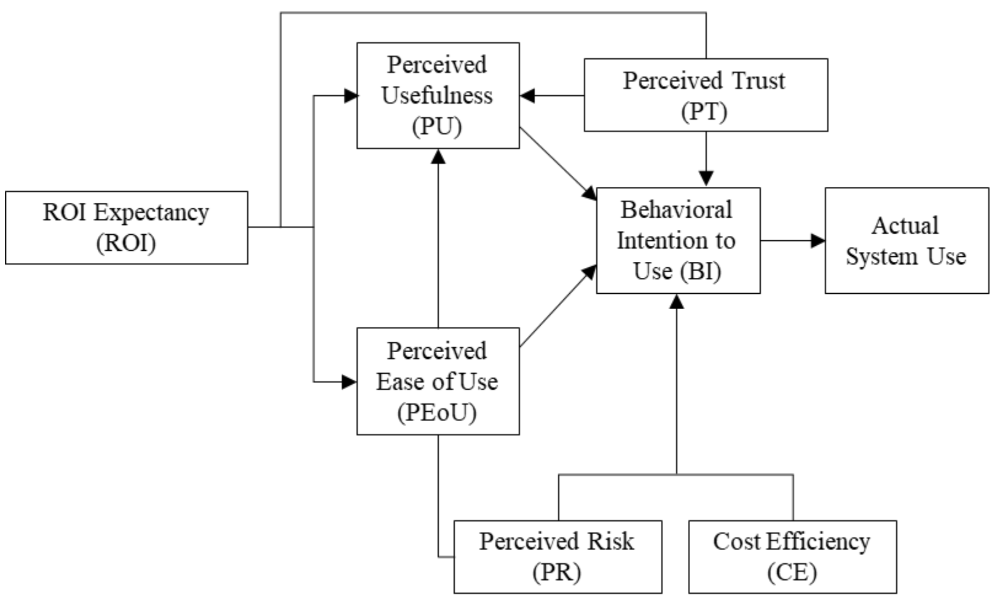


Figure 33 Proposed Theoretical Framework to evaluate the adoption of IIoT users working in Industries

CHAPTER 5

DISCUSSIONS AND CONCLUSION

This section will conclude our study by discussing our findings and evaluating them more comprehensively.

5.1. Discussions

Within the scope of our research, we have conducted a quantitative study with 342 people and a qualitative study with 11 experts. Our qualitative study aimed to hear the core benefits and challenges of IIoT directly from users and form the basis of our quantitative work. Two issues came to the fore in our interviews. First, users suffer from the interoperability of IIoT systems and their integration problems with the existing systems. This situation indicates the lack of standards that can be followed between the system providers. Secondly, users complain about security problems, especially about privacy.

We received responses from 342 people regarding adopting IIoT technology through the survey method on the quantitative side. As we examined in Section 4.5, the number of samples and questions are sufficient to perform the study. The literature shows that most of the technology acceptance models studies are specific to the consumer IoT. Some of these can be listed as technology adoption models tailored to measuring perceptions of intelligent home appliances, wearable intelligent health devices, smart thermostats, smart meters, and mobile phone integrated applications. On the IIoT side, we see that most of the studies are done theoretically, and quantitative measurements are made in a very narrow scope. Gathering information from users on the industrial side of IoT is not easy. The issues that should be considered are the determination of the participant, the company's rules, and the workload of the person we want to participate in the survey. In this respect, our study is essential regarding the number of samples, target audience, and content and fills the gap in this field.

Two hundred fifty-five people from Turkey and 87 from other regions participated in our research. The number of participants who responded to the survey from Turkey can be criticized. At this point, we can state that participation from international regions has increased the depth and diversity of our research.

Evaluation of the hypotheses within the scope of the research is as given in Table 34 below:

Table 34 Evaluation of Hypotheses

Factors	Hypotheses	T Statistics	Evaluation Result
Implications on BI			
Cost Efficiency (CE) → BI_	New	3.337	Supported
Perceived Ease of Use (PEoU) → BI_	H2	2.275	Supported
Perceived Risk (PR) → BI_	H8	4.496	Supported
Perceived Trust (PT) → BI_	H7	3.568	Supported
Perceived Usefulness (PU) → BI_	H1	4.092	Supported
Facilitating conditions (FC) → BI	H9	Grouped with BI	Supported
ROI Expectancy(ROI) → BI_	H6	1.283	Not supported
Implications on Perceived Usefulness			
Perceived Ease of Use → Perceived Usefulness	H3	9.034	Supported
ROI Expectancy → Perceived Usefulness	New	2.353	Supported
Motivation → Perceived Usefulness	H4	Grouped with PEoU	Supported
Compatibility → Perceived Usefulness	H5	Grouped with PT	Supported
Perceived Trust → Perceived Usefulness	New	3.804	Supported
Cost Efficiency → Perceived Usefulness	New	0.265	Not supported
Perceived Risk → Perceived Usefulness	New	0.553	Not supported
Implications on Perceived Ease of Use			
Perceived Risk → Perceived Ease of Use	New	1.995	Supported
Perceived Trust → Perceived Ease of Use	New	6.649	Supported
ROI Expectancy → Perceived Ease of Use	New	2.792	Supported

We can examine the above table in three main sections as follows:

5.1.1. Implications on Behavioral Intention to Use (BI)

PR, composed of cyber-security concerns, the continuous connectivity of all devices to the Internet, and reliability issues, had the most significant impact on BI. In other words, the lower the risk perception, the higher the BI. On the other hand, CE, PT, PU, and PEoU also have significant effects on BI, and the cumulative of these four factors outweigh PR in the emergence of intention to use. An exciting result of the research is that the ROI factor, which includes items such as opening up to new markets, being more competitive, and returning the investment in a short time, did not affect BI. Instead, it is noteworthy that CE, which includes affordability and overweighing the costs by the benefits, influences BI more than ROI.

5.1.2. Implications on Perceived Usefulness (PU)

One of the factors that affect PU is PEoU. As seen in the above table, PEoU has a significant effect on PU, and even this effect is ahead of all interactions. This situation reveals the importance of training activities and the principle of simplicity. As discussed in Section 4.5.4, at least 1.8 is required for the T value to be accepted (Salloum et al., 2019). In this respect, it can be inferred that ROI expectation and PT factors affect PU significantly. However, these two factors seem to have lower PU effects than PEoU. The research revealed that CE and PR did not considerably impact PU, and these two factors affected more direct use.

5.1.3. Implications on Perceived Ease of Use (PEoU)

Among the factors affecting PEoU, PT has the most significant effect. The partners play vital roles throughout IIoT projects by providing seamless interoperability between the systems, integrating the IIoT systems into the legacy systems, producing healthy solutions in case of possible problems, and ensuring the reliability of the data. As discussed in Section - 2.6.8, the choice of organizations in selecting a reputable partner is crucial for the project's health. In addition, ROI expectation and PR also impact PEoU, albeit lower compared to PT.

5.2. Conclusion

In this study, two factors came to the fore with their high impact values. The first is the **perceived risk**, which directly affects the behavioral intention to use IIoT technology negatively. The second is the **perceived trust**, which significantly increases the perception of ease of use and indirectly affects the perceived usefulness.

The results should also be considered in the triangle of security, ease of use (usability), and functionality. In this context, it should be examined how a factor in the triangle affects the decrease or increase in efficiency of the other two elements. As an actual result of the research, it was determined that a change in ease of use directly affects perceived usefulness. In addition, the reduction of security risk increases both ease of use and functionality (Furnell, 2018).

However, there is an inverse interaction between security and functionality in the real world. Increasing security measures can reduce usability in many cases. In this regard, solution providers need to provide an optimum solution (Framling and Nyman, 2008). In this case, as discussed in Section 2.6.6, cyber resilience plays a crucial role in mitigating the risks (Nakamura & Ribeiro, 2018). Increasing cyber resilience should not be limited to identifying vulnerabilities and eliminating threats (Ratasich et al., 2019). Still, it should also include determining the overall security strategy throughout the organization and having high-security awareness of the people (Rajab, Saxena & Salonitis, 2020) who will use the system (Patel & Patel, 2016). On the other hand, no matter how robust an organization's security infrastructure is, problems due to human errors should not be ignored. In this respect, management's support, following the policies and standards, periodical training activities on security must also be considered by the organizations (Nicolescu et al., 2018).

Today, large organizations are under the threat of targeted attacks. There has been a significant increase in these attacks (Panchal, Khadse & Mahalle, 2018). In a possible attack, catastrophic situations may arise to deteriorate human life and environmental health (Mosenia & Jha, 2016). In this case, the organizations can consider artificial intelligence-enabled IDS (intrusion detection prevention) systems and Anti-APT (advanced persistent threat) systems to prevent such situations (Stellios et al., 2018; Hutchins et al., 2011). In addition, blockchain technology, whose value has increased with the IIoT, can also play an active role in enhancing the security standpoint of organizations (Khan & Salah, 2018). Finally, among the security measures, ensuring human safety also plays an important role. However, safety comes after cyber security, reliability, and privacy in the IT world (Moore, Nugent, Zhang & Cleland, 2020). This situation poses a significant risk for the IT and OT worlds (Nakamura & Ribeiro, 2018). To increase safety throughout the company, the sensitivity of the sensors used for measurement at risky points should be very high. In addition, the digital twin can create an essential opportunity in industries that require harsh conditions such as oil and gas refining, iron and steel production, mining. Another problem with security is ensuring privacy (Gebremichael et al., 2020; Sadeghi, Wachmann & Waidner, 2015). Before starting any IIoT project, the stakeholders must contractually decide on the data ownership and define ways to increase cloud security. The edge computing technology described in Section 2.4.3 bears great importance (Hameed, Khan & Hameed, 2018). Additionally, in the future, with the spread of distributed cloud systems (Brody & Pureswaran, 2015), organizations will be able to host the cloud within their structure, and privacy will be ensured to a great extent.

In addition, the trustworthiness of an IIoT system is directly related to the interoperability and integrability and the competencies of the business partners who will commission the system. As determined in literature research and qualitative research, researchers and experts primarily focus on interoperability. As discussed in Section 2.6.1, many IIoT systems have been developed for various usage purposes, and these systems mostly use standards they have set themselves. This heterogeneity situation naturally brings along interoperability and integration problems; therefore, this issue needs to be delicately handled by policy-makers, and solutions should be produced. As one of the solution alternatives, a semantic approach that adopts WEB 3.0 can be applied so that systems can communicate with each other invisibly (Ganzha et al., 2018). As described in Section 2.3.1, next-generation sensors can also be good alternatives in providing easy implementation and instantly starting data collection. In addition, in recent years, there have been significant developments, especially in 3D printing. Thanks to 3D printing, integration points that may cause problems can be reproduced to support IIoT equipment. In this way, integration difficulties can be minimized.

Despite these two critical factors affecting the usage trend, 84% of companies actively use IIoT technology, according to the survey results conducted for 342 participants. This situation reveals that other factors like expectations from an IIoT system and growth strategy may also be necessary for the companies to invest in IIoT technology. In this regard, before purchasing the solutions to be invested in, organizations should evaluate the benefits obtained from the systems in terms of technological, functional, and operational aspects.

5.3. Contribution of the study

This study can contribute to IIoT solution providers, other business partners, end-users, and researchers by providing theoretical and practical information with examples, quantitative and qualitative research methods, and practically applicable results. The study can be adapted to another country or region or applied to a single sector. Moreover, the scope can be extended to identify the influencing usage factors of other IIoT enabled emerging technologies like digital twin, blockchain, AI, 3D printing, and edge computing (Gajek, Lees & Jansen, 2020; Liu et al., 2019). At this point, it should be noted that organizations are particularly uncomfortable with investigating demographic structures such as age and gender or any other subjective norms, and such a situation can significantly reduce the number of samples.

5.4. Limitations of this study

The vast majority of this work was done during the worst pandemic conditions. Since most of the organizations were completely closed or working remotely or part-time, there were some problems, such as the fact that the users who would respond to the survey were not at their workplaces or were extremely busy. In addition, the author has suffered from COVID disease twice during this period. All these factors have caused the author to perform the researches in a limited time.

In addition, the DEMATEL methodology was applied with the participation of 11 experts to identify the influencing factors, but this method was not specified in the study due to time limitations. Lastly, a sector or region-based evaluation of the behavioral intention could not be performed to stick to deadlines.

5.5. Future studies

In the short term, it is aimed to write an academic article about this study, including the effects of sectors and regions on adoption. Since the methods and resources to be followed were determined in this study, new research can be performed with more samples covering a wider area. In the medium term, it is envisaged that a security framework study will be carried out that will satisfy all stakeholders in IIoT technology.

REFERENCES

Ahemd M. M., Shah M. A. and Wahid A. (2017). IoT security: A layered approach for attacks & defenses. *International Conference on Communication Technologies*, 104-110. doi:10.1109/COMTECH.2017.8065757

Ahmed W., Hizam S. M., Sentosa I., Akter H., Yafi E., Jawad A. (2020). Predicting IoT Service Adoption towards Smart Mobility in Malaysia: SEM-Neural Hybrid Pilot Study. *(IJACSA) International Journal of Advanced Computer Science and Applications, 11*(1), 524-535.

Ajzen I. (1985). *From Intentions to Actions: A Theory of Planned Behavior.* Berlin, Heidelberg: Springer. doi:10.1007/978-3-642-69746-3_2

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

Ajzen I. and Fishbein M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin, 82*(2), 261–277. doi:10.1037/h0076477

Al-Emran M., Granić A. (2021). Is It Still Valid or Outdated? A Bibliometric Analysis of the Technology Acceptance Model and Its Applications From 2010 to 2020. In *Recent Advances in Technology Acceptance Models and Theories. Studies in Systems, Decision, and Control* (Vol. 335). Springer, Cham. doi:10.1007/978-3-030-64987-6_1

Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., and Ayyash M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials, 17*(4), 2347-2376. doi:10.1109/COMST.2015.2444095

Ali Z.H., Ali H.A., and Badawy M.M. (2015). Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. (47, Ed.) *International Journal of Computer Applications, 128*(1), 37.

Al-Momani A.M., Mahmoud M.A., Ahmad M.S. (2018). Factors that Influence the Acceptance of Internet of Things Services by Customers of Telecommunication Companies in Jordan. *Journal of Organizational and End User Computing (JOEUC)*. doi:10.4018/JOEUC.2018100104

Al-Qeisi K., Dennis C., Alamanos E., Jayawardhena C. (2014). Website design quality and usage behavior: Unified Theory of Acceptance and Use of Technology.

Journal of Business Research, 67(11), 2282-2290. doi:10.1016/j.jbusres.2014.06.016

Al-Turjman F. and Alturjman S. (2018). Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. *IEEE Transactions on Industrial Informatics, 14*(6), 2736-2744. doi:10.1109/TII.2018.2808190

Alwahaishi S., Snásel V. (2013). Consumers' Acceptance and Use of Information and Communications Technology: A UTAUT and Flow-Based Theoretical Model. *Journal of Technology Management & Innovation, 18*(2). doi:10.4067/S0718-27242013000200005

Amalraj J.J, Banumathi S., John J.J. (2016). IoT Sensors and Applications: A Survey. *International Journal of Scientific & Technology Research, 8*(8).

Anawar M.R., Wang S., Zia M.A., Jadoon A.K., Akram U. and Raza S. (2018). Fog Computing: An Overview of Big IoT Data Analytics. *Wireless Communications and Mobile Computing, 2018*, 22 pages. doi:10.1155/2018/7157192

Ankele R., Marksteiner S., Nahrgang K., Vallant H. (2019). Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis, and Penetration Testing. *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability, and Security, Article: 102*, pp. 1-8. doi:10.1145/3339252.3341482

Annicchino P., Brékine A., Facca F.M., Adriënne H., Castro F.M. (2018). *Next Generation Internet of Things.* NGIoT Consortium 2018-2021. Retrieved from https://www.ngiot.eu/wp-content/uploads/sites/26/2020/09/D3.1.pdf

Arabi K. (2014). Low Power Design Techniques in Mobile Processes. *ISLPED '14: Proceedings of the 2014 International Symposium on Low Power Electronics and Design.* La Jolla, CA, USA: Association for Computing Machinery. doi:10.1145/2627369

Arifin Z., Frmanzah. (2015). The effect of the dynamic capability on technology adoption and its determinant factors for improving firm's performance; toward a conceptual model. *11th International Strategic Management Conference. 207*, pp. 786 – 796. Vienna, Austria: Elsevier Ltd.

Bajaj S. (2018). *Industrial Internet of Things Market Outlook - 2023.* Allied Market Research. Retrieved from https://www.alliedmarketresearch.com/industrial-internet-of-things-IIOT-market

Bajramovic E., Gupta D., Guo Y., Waedt K., and Bajramovic A. (2019). Security Challenges and Best Practices for IIoT. *INFORMATIK 2019 Workshops,* (pp. 243-254). Bonn, Germany. doi:10.18420/inf2019_ws28

Baker J. (2012). The Technology–Organization–Environment Framework. In W. M. Dwivedi Y., & V. S. Sharda R. (Ed.), *Information Systems Theory. Integrated Series in Information Systems* (Vol. 28). Springer. doi:10.1007/978-1-4419-6108-2_12

Bali M., Tari A.A.K., Almutawakel A., Kazar O. (2020). Smart Design for Resources Allocation in IoT Application Service Based on Multi-agent System and DCSP. *Informatica, 44*, 373–386. doi:10.31449/inf.v44i3.2962

Bansal S., Kumar D. (2020). IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware, and Communication. *International Journal of Wireless Information Networks, 27*, 340–364. doi:10.1007/s10776-020-00483-7

Bedhief I., Foschini L., Bellavista P., Kassar M. and Aguili T. (2019). Toward Self-Adaptive Software-Defined Fog Networking Architecture for IIoT and Industry 4.0. *24th International Workshop on Computer-Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-5). Limassol, Cyprus: IEEE. doi:10.1109/CAMAD.2019.8858499

Behrendt A., de Boer E., Kasah T., Koerber B., Mohr N., and Richter G. (2021). *Leveraging Industrial IoT and advanced technologies for digital transformation.* Mc Kinsey & Company.

Bekara C. (2014). Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Computer Science. 34*, pp. 532–537. Elsevier Ltd. doi:10.1016/j.procs.2014.07.064

Bellavista P. and Foschini L. (2020). 04 – Internet of Things (IoT): Definitions and Application Scenarios. Bologna, Italy. Retrieved from http://lia.disi.unibo.it/Courses/sm2021-info/lucidi/04-IoT(2x).pdf

Berte D.R. (2018). Defining the IoT. *Proceedings of the International Conference on Business Excellence. 12*, pp. 118-128. Sciendo. doi:10.2478/picbe-2018-0013

Biswas A.R. and Giaffreda R. (2014). IoT and cloud convergence: Opportunities and challenges. *IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375-376). Seoul, Korea (South): IEEE. doi:10.1109/WF-IoT.2014.6803194

Boer P.S., Deursen A.,and Rompay T. (2018). Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and Informatics*, 147-157. doi:10.1016/j.tele.2018.12.004

Bonett D.G. and Wright T.A. (2014). Cronbach’s alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*. doi:10.1002/job.1960

Boye A.C., Kearney P., and Josephs M. (2018). Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment. In *Information Security. ISC 2018. Lecture Notes in Computer Science* (pp. 502-519). Cham, Switzerland: Springer Publications. doi:10.1007/978-3-319-99136-8_27

Boyes H., Hallaq B., Cunningham J., Watson T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*(101), 1–12. doi:10.1016/j.compind.2018.04.015

Brambilla M., Umuhoza E. and Acerbis R. (2017). Model-driven development of user interfaces for IoT systems via domain-specific components and patterns. *Journal of Internet Services and Applications, 8*(14). doi:10.1186/s13174-017-0064-1

Brody P. and Pureswaran V. (2015). The next digital gold rush: how the internet of things will create liquid, transparent markets. *Strategy and Leadership, 43*(1), 36-41. doi:10.1108/SL-11-2014-0094

Brunner M. and Süβ M.H. (2005, April). Analyzing the Reliability of Multidimensional Measures: An Example from Intelligence Research. *Educational and Psychological Measurement, 65*(2), 227-239. doi:10.1177/0013164404268669

Cabral L.M.B., Salant D.J. and Woroch G.A. (1999, February). Monopoly pricing with network externalities. *International Journal of Industrial Organization, 17*(2), 199-214. doi:10.1016/S0167-7187(97)00028-3

Cao H., Wachowicz M., Renso C. and Carlini E. (2019). Analytics Everywhere: Generating Insights From the Internet of Things. *IEEE Access*. doi:10.1109/ACCESS.2019.2919514

Castle J.L, Qin X., and Reed W.B. (2011). Using Model Selection Algorithms to Obtain Reliable Coefficient Estimates. *Journal of Economic Surveys*, 269-296. doi:10.1111/j.1467-6419.2011.00704.x

Chang A. (2012). UTAUT and UTAUT 2: A Review and Agenda for Future Research. (A. R., Ed.) *The Winners, 13*(2). doi:10.21512/tw.v13i2.656

Chatterjee S., Rana N.P., Dwivedi Y.K. and Baabdullah A.M. (2021, September). Understanding AI adoption in manufacturing and production firms using an integrated TAM-TOE model. *Technological Forecasting & Social Change, 170*. doi:10.1016/j.techfore.2021.120880

Chin W.W. (1998, March). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly, 22*(1), 7-17. Retrieved from http://www.jstor.org/stable/249674

Chowdhury A. and Raut S.A. (2019). Benefits, Challenges, and Opportunities in Adoption of Industrial IoT. *International Journal of Computational Intelligence & IoT, 2*(4). Retrieved from https://ssrn.com/abstract=3361

Cisco. (2017). *Close to Three-Fourths of IoT Projects Are Failing.* Retrieved from Cisco.com: https://newsroom.cisco.com/press-release-content?articleId=1847422

Colakovic A. and Hadzialic M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144*, 17-39. doi:10.1016/j.comnet.2018.07.017

Conway J. (2015). *The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise.* Schneider Electric. Retrieved from https://www.semanticscholar.org/paper/The-Industrial-Internet-of-Things-%3A-An-Evolution-to-Conway/7c944c548be9cde1b96598344b28ca6117106c96

Cook A., Maglaras L., Smith R. and Janicke H. (2018). Managing incident response in the industrial internet of things. *International Journal of Internet Technology and Secured Transactions*, *8*(2). doi:10.1504/IJITST.2018.093336

Cronbach L.J. (1951, September). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. doi:10.1007/BF02310555

Cronbach L.J. and Meehl P.E. (1955). Construct validity in psychological tests. *Psychological Bulletin, 52*(4), 281–302. doi:10.1037/h0040957

CTI Group. (n.d.). *www.computradetech.com*. Retrieved 11 1, 2021, from IoT vs. IIoT: https://www.computradetech.com/blog/iot-vs-iiot/

Daji D., Ghule K., Gagdani S., Butala A., Talele P. and Kamat H. (2020). Cloud-Based Asset Monitoring and Predictive Maintenance in an Industrial IoT System. *International Conference for Emerging Technology (INCET)* (pp. 1-5). Belgaum, India: IEEE. doi:10.1109/INCET49848.2020.9154148

Davis F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340. doi:10.2307/249008

Davis F.D. and Venkatesh V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies, 45*(1), 19-45. doi:10.1006/ijhc.1996.0040

Dewan S. and Riggins J.F. (2005). The Digital Divide: Current and future research directions. *Journal of the Association for Information Systems*.

Dhirani L.L., Newe T., and Nizamani S. (2018). Can IoT escape Cloud QoS and Cost Pitfalls. *12th International Conference on Sensing Technology (ICST)* (pp. 65-70). Limerick, Ireland: IEEE. doi:10.1109/ICSensT.2018.8603570

Dhirani L.L., Armstrong E., and Newe T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Science*. MDPI. doi: 1424-8220/21/11/3901

Disruptive Technologies. (2021, November 6). *Disruptive Technologies*. Retrieved from https://www.disruptive-technologies.com/

Drazin R. (1991, March). The processes of technological innovation. *The Journal of Technology Transfer*, *16,* 45-46. doi:10.1007/BF02371446

Eckhardt A., Laumer S. and Weitzel T. (2009, March). Who influences whom? Analyzing workplace referents' social influence on its adoption and non-adoption. *Journal of Information Technology*, *24,* 11-24. doi:10.1057/jit.2008.31

El-Masri M. and Tarhini A. (2017). Factors affecting the adoption of e-learning systems in Qatar and USA: Extending the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2). *Educational Technology Research and Development, 65*, 743–763. doi:10.1007/s11423-016-9508-8

Evans D. (2011). *How the Next Evolution of the Internet Is Changing Everything?* Cisco. Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Evans L. and Donnellan B. (2015). Unpacking the 'Thing' in the Internet of Things. *Pre-ICIS Workshop 2015*, (p. 10 pages). Retrieved from https://cris.brighton.ac.uk/ws/files/398785/SIGPRAG2015-LE-BD.pdf

Field A. (2013). *Discovering Statistics Using IBM SPSS Statistics* (4th ed.). (C. M., Ed.) London: Sage Publications. doi:10.5555/2502692

Fishbein M., Jaccard J., Davidson A. R., Ajzen I. and Loken B. (1980). Predicting and understanding family planning behaviors. In &. M. Ajzen, *Understanding attitudes and predicting social behavior.* Prentice-Hall.

Flick U. (2018). *Designing Qualitative Research.* (S. M., Ed.) Sage Publications Ltd.

Fornell C. and Larcker D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. doi:10.1177/002224378101800104

Forsström S., Butun I., Eldefrawy M., Jennehag U. and Gidlund M. (2018). Challenges of Securing the Industrial Internet of Things Value Chain. *Workshop on Metrology for Industry 4.0 and IoT*, 218-223. doi:10.1109/METROI4.2018.8428344

Foukalas F., Pop P., Theoleyre F., Boano C.A., and Buratti C. (2019). Dependable Wireless Industrial IoT Networks: Recent Advances and Open Challenges. *IEEE European Test Symposium (ETS)* (pp. 1-10). Baden-Baden, Germany: IEEE. doi:10.1109/ETS.2019.8791551

Fraile F., Tagawa T., Poler R., and Ortiz A. (2018). Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems. *IEEE Internet of Things Journal, 5*(6), 4506-4514. doi:10.1109/JIOT.2018.2832041

Frambach R.T. and Schillewaert N. (2002). Organizational innovation adoption: a multi-level framework of determinants and opportunities for future research. *Journal of Business Research, 55*(2), 163-176. doi:10.1016/S0148-2963(00)00152-1

Framling K., and Nyman J. (2008). The compromise between Security and Usability in the Internet of Things. Researchgate accessed on November 21st, 2021 at https://www.researchgate.net/publication/228982745

Friedman J. and Goldstein B. (2019, July). IoT Suffers from a Lack of Standards. *Printed Circuit Design & FAB*, *37*(7), 30-31. Retrieved from https://www.upmediagroup.net/publications/2007PCDFCA.pdf

Furnell S. (2018). Trust, Privacy, and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5-6, 2018, Proceedings. Springer Publications, Cham, Switzerland. doi: 10.1007%2F978-3-319-98385-1

Gajek S., Lees M. and Jansen C. (2021). IIoT and cyber-resilience. AI & Society, 36, 725–735. doi:10.1007%2Fs00146-020-01023-w

Ganzha M. et al. (2018). Towards Semantic Interoperability Between the Internet of Things Platforms. In G. R. al., *Integration, Interconnection, and Interoperability of IoT Systems* (pp. 103-128). Springer International Publishing AG 2018. doi:10.1007/978-3-319-61300-0

Gartner. (2016). *Survey Analysis: 2016 Internet of Things Backbone Survey*. Gartner. Retrieved from https://www.gartner.com/en/documents/3563218/survey-analysis-2016-internet-of-things-backbone-survey

Gartner. (2021). *Leading IoT.* Gartner. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf adresinden alındı

Gebremichael T. et al. (2020, August). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access, 8*, 152351-152366. doi:10.1109/ACCESS.2020.3016937

Gilchrist A. (2016). *Industry 4.0: The Industrial Internet.* (P. J., Ed.) Apress. doi:10.1007/978-1-4842-2047-4

Gliem J.A. and Gliem R.R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. *Midwest Research to Practice Conference in Adult, Continuing, and Community Education* (pp. 82-88). The Ohio State University. Retrieved from https://scholarworks.iupui.edu/handle/1805/344

Gochhayat, S.P., Lal, C., Sharma, L. et al. (2020). Reliable and secure data transfer in IoT networks. *Wireless Networks, 26*, 5689–5702. doi:10.1007/s11276-019-02036-0

Gotmare A. and Bokate S. (2019). Internet of Things in Manufacturing: A Review on Applications, Challenges, and Future Directions. *5th International Conference on Industrial Engineering (ICIE-2019)*, (p. 9 pages). Surat, India.

Goundar S., Bhardwaj A., Nur S.S., Kumar S.S., and Harish R. (2021). Industrial Internet of Things: Benefit, Applications, and Challenges. In G. S. al., *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory* (pp. 133-148). IGI Global. doi:10.4018/978-1-7998-3375-8.ch010

Grandview Research Company, report. (n.d.). *Internet Of Things Market Size, Share & Trends Report*. Retrieved 11 1, 2021, from www.grandviewresearch.com/: https://www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market

Gravina R. et al. (2018). *Integration, Interconnection, and Interoperability of IoT Systems.* (R. G. A., Dü.) Cham, Switzerland: Springer International Publishing AG. doi:10.1007/978-3-319-61300-0

Guggenberger T.M., Hunke F., Möller F., Eimer AC., Satzger G. and Otto B. (2021). How to Design IIoT-Platforms Your Partners are Eager to Join: Learnings from an Emerging Ecosystem. In S. R. Ahlemann F., & S. S. (Ed.), *Innovation Through Information Systems* (Vol. 48, pp. 489-504). Cham, Switzerland: Springer. doi:10.1007/978-3-030-86800-0_34

Gupta A., Reddy V.B. and Solanki H.K. (2018). Cost in high impact journals: The problem for researchers from low and middle-income countries. *International Journal of Public Health Research, 5*(1), 45-49. doi:10.17511/ijphr.2018.i1.06

Hair J. F. (2009). *Multivariate Data Analysis: A Global Perspective.* (7th ed.). Upper Saddle River: Prentice-Hall.

Hale J., Householder B. and Green K. (2002). The Theory of Reasoned Action. In D. J. M., *The persuasion handbook: developments in theory and practice* (pp. 259-263). SAGE Publications. doi:10.4135/9781412976046

Hameed S., Khan F.I. and Hameed B. (2019, January). Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. (S. D.F.H, Ed.) *Journal of Computer Networks and Communications*, 19 pages. doi:10.1155/2019/9629381

Haradhan K.M. (2019). The First Industrial Revolution: Creation of New Global Human Era. *Journal of Social Sciences and Humanities, 5*(4), 377-387. Retrieved from https://mpra.ub.uni-muenchen.de/96644/

Hassanzadeh A., Modi S., and Mulchandani S. (2015). Towards effective security control assignment in the Industrial Internet of Things. *IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 795-800). Milan, Italy: IEEE. doi:10.1109/WF-IoT.2015.7389155

Hassija V., Chamola V., Saxena V., Jain D., Goyal P., and Sikdar B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access, 7*, 82721-82743. doi:10.1109/ACCESS.2019.2924045

Hermann M., Pentek T. and Otto B. (2016). Design Principles for Industrie 4.0 Scenarios. *49th Hawaii International Conference on System Sciences* (pp. 3927-3937). IEEE. doi:10.1109/HICSS.2016.488

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

Huang C.C., Wang Y.M., Wu T.W. and Wang P.A. (2013). An Empirical Analysis of the Antecedents and Performance Consequences of Using the Moodle Platform. *International Journal of Information and Education Technology, 3*(2), 217-222. doi:10.7763/IJIET.2013.V3.267

Hutchins E.M., Cloppert M.J. and Amin R.M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In R. J. (Ed.), *Leading Issues in Information Warfare & Security Research* (Vol. 1). Academic Conferences Limited.

IDC Report. (2021). Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS47560321

IHS Report. (2016). *IoT Platforms: Enabling the Internet of Things.* IHS Technology. Retrieved 11 1, 2021, from https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

Industrial Internet Consortium. (2016). *Industrial Internet of Things Volume G4: Security Framework.* Industrial Internet Consortium. Retrieved from https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

IoT Nexus Survey. (n.d.). *77% of IoT Professionals see Interoperability as the biggest challenge facing IoT | FC Business Intelligence Survey*. Retrieved from www.prweb.com: https://www.prweb.com/releases/2015/02/prweb12535904.htm

Isaac O., Abdullah Z. and Ramayah T. (2016). Perceived Usefulness, Perceived Ease of Use, Perceived Compatibility, and Net Benefits: an empirical study of internet usage among employees in Yemen. *7th International Conference on Postgraduate Education*, (pp. 899–919). Malaysia.

Jangid A. and Chauhan P. (2019). A Survey and Challenges in IoT Networks. *International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 516-521). Palladam, India: IEEE. doi:10.1109/ISS1.2019.8908079

Junglas I.A. and Spitzmuller C. (2005). A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (pp. 180b-180b). Big Island, HI, USA: IEEE. doi:10.1109/HICSS.2005.47

Kamal S.Z., Al Mubarak S.M., Scodova B.D., Naik P. Flichy P. and Coffin G. (2016). IT and OT Convergence - Opportunities and Challenges. *SPE Intelligent Energy International Conference and Exhibition* (pp. SPE-181087-MS). Aberdeen, Scotland, UK: Society of Petroleum Engineers (SPE). doi:10.2118/181087-MS

Kao Y.S., Nawata K. and Huang C.Y. (2019). An Exploration and Confirmation of the Factors Influencing Adoption of IoT-Based Wearable Fitness Trackers. *Int. J. Environ. Res. Public Health*, 3227. doi:10.3390/ijerph16183227

Karanja E.M., Masupe S., and Mandu J. (2017). Internet of Things Malware: A Survey. *International Journal of Computer Science & Engineering Survey (IJCSES)*, *8*, p. 20 pages. doi:10.5121/ijcses.2017.8301

Kassab M., D. J. (2019). A systematic literature review on Internet of things in education: Benefits and challenges. *Journal of Computer Assisted Learning, 36*(2), 115-127. doi:10.1111/jcal.12383

Kauffman R.J. and Walden E.A. (2001). Economics and Electronic Commerce: Survey and Directions for Research. *International Journal of Electronic Commerce, 5*(4), 5-116. doi:10.1080/10864415.2001.11044222

Kenny D.A. (2021, 11 5). *Measuring Model Fit*. Retrieved from http://www.davidakenny.net/: http://www.davidakenny.net/cm/fit.htm

Khalil R.A., Saeed N., Masood M., Fard Y.M., Alouini M.S., and Al-Naffouri T.Y. (2021). Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications. *IEEE Internet of Things Journal, 8*(14), 11016-11040. doi:10.1109/JIOT.2021.3051414

Khan M.A. and Salah K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*(82), 395–411. doi:10.1016/j.future.2017.11.022

Khan W.Z. and Khan M.K. (2019). *Advanced Persistent Threats Through Industrial IoT On Oil And Gas Industry*. Global Foundation for Cyber Studies and Research. Retrieved from https://www.researchgate.net/publication/335611873_Advanced_Persistent_Threats_Through_Industrial_IoT_On_Oil_And_Gas_Industry

Khatimah H., Susanto P. and Abdullah N.L. (2019). Hedonic motivation and social influence on behavioral intention of e-money: The role of payment habit as a mediator. *International Journal of Entrepreneurship, 23*(1), 1-9.

Khodadadi F., Dastjerdi A.V., and Buyya R. (2016). Chapter 1 - Internet of Things: an overview. In K. M., *Kaufmann* (pp. 3-27). ScienceDirect. doi:10.1016/B978-0-12-805395-9.00001-0

Kim D.S., and Dang H.T. (2020). Reliability Evaluation Model Of Industrial Internet Of Things Systems. *1st International Conference on Engineering (ICONE 2020)*, (pp. 1-3). doi:10.36728/icone.v1i1.1266

King W.R. and He J. (2006). A meta-analysis of the technology acceptance model. *Information & Management, 43*(6), 740-755. doi:10.1016/j.im.2006.05.003

Kocaleva M., Stojanovic I. and Zdravev Z. (2015). Model of e-Learning Acceptance and Use for Teaching Staff in Higher Education Institutions. *I.J. Modern Education and Computer Science, 4*, 23-31. doi:10.5815/ijmecs.2015.04.03

Kock N. (2016). Hypothesis Testing with Confidence Intervals and P Values in PLS-SEM. *IGI Global*, 6 pages. doi:10.4018/IJeC.2016070101

Kusiak A. (2018). Smart manufacturing. *International Journal of Production Research, 56*(1-2), 508-517. doi:10.1080/00207543.2017.1351644

Lafreniere K.C., Hunter M.G. and Deshpande S. (2011). Comparing and Prioritizing the Factors Affecting Purchase Decisions in Innovation Adoption in a Post-Secondary

Educational Setting. *Journal of Information, Information Technology, and Organizations, 6*(2011-2012), 15-39. doi:10.28945/1557

Lampropoulos G., Siakas K. and Anastasiadis T. (2019). Internet of THings in the context of Industry 4.0: An Overview. *International Journal of Entrepreneurial Knowledge, 7*(1), 4-19. doi:10.37335/ijek.v7i1.84

Laroca R. et al. (2018). A Robust Real-Time Automatic License Plate Recognition Based on the YOLO Detector. *International Joint Conference on Neural Networks (IJCNN)* (pp. 1-10). Rio de Janeiro, Brazil: IEEE. doi:10.1109/IJCNN.2018.8489629

Lee I. and Lee K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440. doi:10.1016/j.bushor.2015.03.008

Li S., Xu L.D. and Zhao S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration, 10,* 1-9. doi:10.1016/j.jii.2018.01.005

Liao Y., Loures E.F.R. and Deschamps F. (2018, December). Industrial Internet of Things: A Systematic Literature Review and Insights. *IEEE Internet of Things Journal, 5*(6), 4515-4525. doi:10.1109/JIOT.2018.2834151

Liedtka J.M. (1992). Exploring Ethical Issues Using Personal Interviews. *Business Ethics Quarterly, 2*(2), 161-181. doi:10.2307/3857569

Linda K., Claire B., Vincent H., Henrica D., and Allard V. (2014). Construct Validity of the Individual Work Performance Questionnaire. *Journal of Occupational and Environmental Medicine, 56*(3), 331-337. doi:10.1097/JOM.0000000000000113

Liu M., Yu F.R., Teng Y., Leung V.C.M. and Song M. (2019, June). Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach. *IEEE Transactions on Industrial Informatics, 15*(6), 3559-3570. doi:10.1109/TII.2019.2897805

López P., Fernández D., Jara A.J. and Skarmeta A.F. (2013). Survey of Internet of Things Technologies for Clinical Environments. *27th International Conference on Advanced Information Networking and Applications Workshops* (pp. 1349-1354). Barcelona, Spain: IEEE. doi:10.1109/WAINA.2013.255

Lukač D. (2015). The fourth ICT-based industrial revolution "Industry 4.0" — HMI and the case of CAE/CAD innovation with EPLAN P8. *23rd Telecommunications Forum Telfor (TELFOR)* (s. 835-838). Belgrade, Serbia: IEEE. doi:10.1109/TELFOR.2015.7377595

Madugula L. (2021, July). Applications of IoT in Manufacturing: Issues and Challenges. *Journal of Advanced Research in Embedded System, 1&2,* 3-7. doi:10.24321/2395.3802.202101

Magomadov V.S. (2020). The Industrial Internet of Things as one of the main drivers of Industry 4.0. *IOP Conference Series: Materials Science and Engineering. 862*, p. 4 pages. IOP Publishing Ltd. doi:10.1088/1757-899X/862/3/032101

Makrakis G.M., Kolias C., Kambourakis G., Rieger C. and Benjamin J. (2021, September 10). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. eprint arXiv:2109.03945. Retrieved from https://arxiv.org/abs/2109.03945

Malatji W.R., Eck R.V. and Zuva T. (2020). Understanding the usage, Modifications, Limitations, and Criticisms of Technology Acceptance Model (TAM). *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 113-117. doi:10.25046/aj050612

Malik B.H., Cheema S.N., Iqbal I., Mahmood Y., Ali M. and Mudasser A. (2018). From Cloud Computing to Fog Computing (C2F): The key technology provides services in health care big data. *2nd International Conference on Material Engineering and Advanced Manufacturing Technology (MEAMT 2018)* (p. 7 pages). MATEC Web Conf. doi:10.1051/matecconf/201818903010

Man S.S., Xiong W., Chang F., and Chan A.H.S. (2020). Critical Factors Influencing Acceptance of Automated Vehicles by Hong Kong Drivers. *IEEE Access, 8,* 109845-10985. doi:10.1109/ACCESS.2020.3001929

Manditereza K. (2017, June 8). 4 Key Differences Between SCADA and Industrial IoT. Retrieved from https://www.linkedin.com/pulse/4-key-differences-between-scada-industrial-iot-kudzai-manditereza/

Mathers N., Fox N. and Hunn A. (1998). *Using Interviews in a Research Project.* Trent Focus Group. Retrieved from http://faculty.cbu.ca/pmacintyre/course_pages/MBA603/MBA603_files/UsingInterviews.pdf

Menezes B.C., Kelly J.D., Leal A.G., Le Roux G.C. (2019). Predictive, Prescriptive and Detective Analytics for Smart Manufacturing in the Information Age. *IFAC-PapersOnLine, 52*(1), 568-573. doi:10.1016/j.ifacol.2019.06.123

Microsoft & Hypothesis. (October 2021). *IoT Signals Edition 3.* Microsoft. Retrieved from https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT%20Signals_Edition%203_English.pdf

Mimecast Report. (2021). *Securing the Enterprise in the COVID world.* Mimecast. Retrieved from https://www.mimecast.com/state-of-email-security/

Mital M., Choudhary P., Chang V., Papa A., and Pani A.K. (2017). Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting & Social Change*, 8 pages. doi:10.1016/j.techfore.2017.03.001

Momani A.M. and Jamous M. (2017, March). The Evolution of Technology Acceptance Theories. *International Journal of Contemporary Computer Research (IJCCR)*, 51-58. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2971454

Moore D., Paxson D., Savage S., Shannon C., Staniford S. and Weaver N. (2003). Inside the Slammer worm. *IEEE Security & Privacy, 1*(4), 33-39. doi:10.1109/MSECP.2003.1219056

Moore S.J., Nugent C.D., Zhang S. and Cleland I. (2020). IoT reliability: a review leading to 5 key research directions. *CCF Transactions on Pervasive Computing and Interaction, 2*, 147-163. doi:10.1007/s42486-020-00037-z

Mordor Intelligence. (2021, 11 01). *IoT Market - Growth, Trends, COVID-19 Impact, and Forecast*. Retrieved from www.mordorintelligence.com: https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry

Morienyane L.D., and Marnewick A. (2019). Technology Acceptance Model of Internet of Things for Water Management at a local municipality. *IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 1-6). Atlanta, GA, USA: IEEE. doi:10.1109/TEMSCON.2019.8813633

Mosenia A. and Jha N.K. (2016). A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586-602. doi:10.1109/TETC.2016.2606384

Moser A. and Korstjens I. (2017, December). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice, 24*, 9-18. doi:10.1080/13814788.2017.1375091

Moura R., Ceotto L., Gonzalez A. and Toledo R. (2018). Industrial Internet of Things (IIoT) Platforms - An Evaluation Model. *International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 1002-1009). Las Vegas, NV, USA: IEEE. doi:10.1109/CSCI46756.2018.00194

Nakamura E.T. and Ribeiro S.L. (2018). A Privacy, Security, Safety, Resilience, and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to

Build and Use Secure IIoT Systems. *Global Internet of Things Summit (GIoTS)* (pp. 1-6). Bilbao, Spain: IEEE. doi:10.1109/GIOTS.2018.8534521

Narayanan K. (2017). *Addressing The Challenges Facing IoT Adoption.* Keysight Technologies. Retrieved from https://www.keysight.com/us/en/assets/7018-05630/article-reprints/5992-2125.pdf

Nicolescu R., Huth M., Radanliev P. and De Roure D. (2018). *State of the Art in IoT - Beyond Economic Value.* London, the UK: Imperial College London. doi:10.13140/RG.2.2.24165.45289

Nunnally J.C., and Bernstein I H. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

O'Connor P.T.D and Kleyner A. (2012). *Practical Reliability Engineering* (3rd ed.). John Wiley & Sons, Ltd. doi:10.1002/9781119961260

O'Keefe C. (2020). *How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents.* Oxford, the UK: University of Oxford. Retrieved from https://www.fhi.ox.ac.uk/wp-content/uploads/How-Will-National-Security-Considerations-Affect-Antitrust-Decisions-in-AI-Cullen-OKeefe.pdf

Opitz N., Langkau T.F. , Schmidt N.H. and Kolbe L.M. (2012). Technology Acceptance of Cloud Computing: Empirical Evidence from German IT Departments. *45th Hawaii International Conference on System Sciences* (pp. 1593-1602). Maui, HI, USA: IEEE. doi:10.1109/HICSS.2012.557

Padmavathi G. and Shanmugapriya D. (2009, August). A Survey of Attacks, Security Mechanisms, and Challenges in Wireless Sensor Networks. *(IJCSIS) International Journal of Computer Science and Information Security*, *4*(1&2), 9 pages. Retrieved from https://arxiv.org/abs/0909.0576

Panchal A.C., Khadse V.M. and Mahalle P.N. (2018). Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. *IEEE Global Conference on Wireless Computing and Networking (GCWCN)* (pp. 124-130). Lonavala, India: IEEE. doi:10.1109/GCWCN.2018.8668630

Parpala R.D. and Iacob R. (2017). Application of IoT concept on predictive maintenance of industrial equipment. *8th International Conference on Manufacturing Science and Education – MSE 2017 "Trends in New Industrial Revolution." 121*, p. 8 pages. EDP Sciences. doi:10.1051/matecconf/201712102008

Patel K. and Patel S. (2016). Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*, 6122-6132.

Retrieved from http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf

Patton M.Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed.). Thousand Oaks, California, USA: Sage Publications.

Perwej Y., Haq K., Parwej F. and Hassan M.M.M. (2019). The Internet of Things (IoT) and its Application Domains. *International Journal of Computer Applications, 182*(49), 35-50. Retrieved from https://www.researchgate.net/profile/Dr-Yusuf-Perwej/publication/332374473_The_Internet_of_Things_IoT_and_its_Applicati on_Domains/links/5cb245afa6fdcc1d49931068/The-Internet-of-Things-IoT-and-its-Application-Domains.pdf

Petrik D. and Herzwurm G. (2020). Towards the IIoT Ecosystem Development - Understanding the Stakeholder Perspective. *28th European Conference on Information Systems.* Marrakesh, Morocco: Researchgate. Retrieved from https://www.researchgate.net/publication/341234513_Towards_the_IIoT_Ecosys tem_Development_-_Understanding_the_Stakeholder_Perspective

Pison F.J.M., Urraca R., Quintian H. and Corchado E. (2017). *Hybrid Artificial Intelligent Systems.* La Rioja, Spain: Springer International Publishing. doi:10.1007%2F978-3-319-59650-1

Pizoń J., Kłosowski K. and Lipski J. (2019). Key role and potential of Industrial Internet of Things (IIoT) in modern production monitoring applications. *III International Conference of Computational Methods in Engineering Science (CMES'18). 252.* EDP Sciences. doi:10.1051/matecconf/201925209003

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014). PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications. *International Journal of Distributed Sensor Networks, 2014,* 14 pages. doi:10.1155/2014/357430

PWC Report, Rimmer A. (2017). *Lead or lag? What the Industrial Internet of Things means for deals.* PwC research and analysis.

Qin X., Shi Y., Lyu K. and Mo Y. (2020). Using a TAM-TOE Model to Explore Factors of Building Information Modelling (BIM) Adoption in the Construction Industry. *Journal of Civil Engineering and Management, 26*(3), 259-277. doi:10.3846/jcem.2020.12176

Rahman F.B.A., Hanafiah M.H.M., Zahari M.S.M. and Jipiu L.B. (2021). Systematic Literature Review on The Evolution of Technology Acceptance and Usage Model used in Consumer Behavioural Study. *International Journal of Academic Research in Business and Social Sciences, 11*(13), 272-298. doi:10.6007/IJARBSS/v11-i13/8548

Rajab S., Saxena P. and Salonitis K. (2020). A Multi-Level Analysis of the Implementation of Industrial Internet of Things: Challenges and Future Prospects. *9th International Conference on Through-life Engineering Service* (p. 8 pages). Cranfield UK: SSRN. doi:10.2139/ssrn.3718005

Ramdani B.,and Kawalek P. (2007). SME Adoption of Enterprise Systems in the Northwest of England. In W. D. McMaster T. (Ed.), *Organizational Dynamics of Technology-Based Innovation: Diversifying the Research Agenda*. Boston, MA, USA: Springer Publications. doi:10.1007/978-0-387-72804-9_27

Ratasich D., Khalid F., Geissler F., Grosu R., Shafique M., and Bartocci E. (2019). A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems. *IEEE Access, 7*, 13260-13283. doi:10.1109/ACCESS.2019.2891969

Reddy B.R., and Sujith A.V.L.N. (2017). A Comprehensive Literature Review on Data Analytics in IIoT. 2757- 2764. doi:10.29042/2018-2757-2764

Renaud K, and Biljon J.V. (2008). Predicting technology acceptance and adoption by the elderly: a qualitative study. *Annual Conference of the South African Institute of Computer Scientists and Information Technologists.* Wilderness, South Africa: Association for Computing Machinery. doi:10.1145/1456659.1456684

Riasanow, T., Jäntgen, L., Hermes, S. et al. (2021, March). Core, intertwined, and ecosystem-specific clusters in platform ecosystems: analyzing similarities in the digital transformation of the automotive, blockchain, financial, insurance, and IIoT industry. *Electron Markets*, 89–10. doi:10.1007/s12525-020-00407-6

Rogers E.M. (1963). What are innovators like? *Theory Into Practice, 2*(5), 252-256. doi:10.1080/00405846309541872

Sadeghi A., Wachsmann C., and Waidner M. (2015). Security and privacy challenges in the industrial Internet of Things. *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). San Francisco, CA, USA: IEEE. doi:10.1145/2744769.2747942

Sahu C.K., Pattnayak S.B., Behera S., and Mohanty M.R. (2020). A Comparative Analysis of Deep Learning Approach for Automatic Number Plate Recognition. *Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC)* (pp. 932-937). Palladam, India: IEEE. doi:10.1109/I-SMAC49090.2020.9243424

Saleem J., Hammoudeh M., Raza U., Adebisi B., and Ande R. (2018). IoT standardization: challenges, perspectives, and solutions. *ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed System* (pp. 1-9). ACM Digital Library. doi:10.1145/3231053.3231103

Salloum S.A., Alhamad A.Q.M., Al-Emran M., Monem A.A., and Shaalan K. (2019). Exploring Students' Acceptance of E-Learning Through the Development of a Comprehensive Technology Acceptance Model. *IEEE Access*, 128445-128462. doi:10.1109/ACCESS.2019.2939467

Sandrić B., and Jurčević M. (2018). Metrology and Quality Assurance in the Internet of Things. *First International Colloquium on Smart Grid*, (pp. 1-6). Retrieved from https://www.researchgate.net/profile/Marko_Jurcevic/publication/325493356_Metrology_and_quality_assurance_in_internet_of_things/links/5bbcf841a6fdcc9552dcf76b/Metrology-and-quality-assurance-in-internet-of-things.pdf

Sarstedt M., Ringle C.M., and Hair J.F. (2017). *Partial Least Squares Structural Equation Modeling.* Hamburg, Germany: Springer International Publishing AG. doi:10.1007/978-3-319-05542-8_15-1

Seetharaman A., Patwa N., Saravanan A.S., and Sharma A. (2019). Customer expectation from Industrial Internet of Things (IIOT). *Journal of Manufacturing Technology Management, 30*(8). doi:10.1108/JMTM-08-2018-0278

Sekar K., Shah S.A., Antony Athithan A.,and Mukil A. (n.d.). Role of Machine Learning Approaches in Remaining Useful Prediction: A Review. In H. S. Peng SL. (Ed.), *Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems* (Vol. 248). Singapore: Springer. doi:10.1007/978-981-16-3153-5_39

Sengupta J., Ruj S., and Das Bit S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 21 pages. doi:10.1016/j.jnca.2019.102481

Serpanos D., and Wolf M. (2018). *Internet of Things (IoT) Systems.* Cham, Switzerland: Springer International Publishing AG. doi:10.1007/978-3-319-69715-4

Shi W., Cao J., Zhang O., Li Y., and Xu L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal, 3*(5), 637-646. doi:10.1109/JIOT.2016.257919

Singh A., and Viniotis Y. (2017). Resource allocation for IoT applications in cloud environments. *International Conference on Computing, Networking, and Communications (ICNC)* (pp. 719-723). Silicon Valley, CA, USA: IEEE. doi:10.1109/ICCNC.2017.7876218

Singh I., Centea D., and Elbestawi M. (2019). IoT, IIoT, and Cyber-Physical Systems Integration in the SEPT Learning Factory. *9th Conference on Learning Factories. 31*, pp. 116-122. Elsevier. doi:10.1016/j.promfg.2019.03.019

Sisinni E., Saifullah A., Han S., Jennehag U., and Gidlund M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724-4734. doi:10.1109/TII.2018.2852491

Soni D., and Makwana A. (2017). A Survey on MQTT: A protocol of Internet of Things (IoT). *ICTPACT - 2017*, (p. 6 pages).

Sopapradit S., and Yoosomboon S. (2019). Acceptance of Technology Digital Twin for learning in the 21st Century. *International Journal of Computer and Information Technology, 8"*(5), 4 pages.

Stankovski S., Ostojic G., Baranovski I., Babic M., and Stanojevic M. (2020). The impact of edge computing on industrial automation. *19th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-4). East Sarajevo, Bosnia and Herzegovina: IEEE. doi:10.1109/INFOTEH48170.2020.9066341

Stellios I., Kotzanikolaou P., Psarakis M., Alcaraz C. and Lopez J. (2018, July). A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495. doi:10.1109/COMST.2018.2855563

Streiner D.L., Norman G.R., and Cairney J. (2015). Introduction to health measurement scales. In *Health Measurement Scales: A practical guide to their development and use* (5th ed., p. Chapter 1). Oxford University Press. doi:10.1093/med/9780199685219.003.0001

Taherdoost H. (2018). A review of technology acceptance and adoption models and theories. *22*, pp. 960-967. Procedia Manufacturing. doi:10.1016/j.promfg.2018.03.137

Tamilmani K., Rana N., Dwivedi Y. (2017). A Systematic Review of Citations of UTAUT2 Article and Its Usage Trends. *16th Conference on e-Business, e-Services, and e-Society*, (pp. 38-49). Delhi, India. doi:10.1007/978-3-319-68557-1_5

Tange K., De Donno M., Fafoutis X., and Dragoni N. (2020). A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Communications Surveys & Tutorials*, *22*(4), 2489-2520. doi:10.1109/COMST.2020.3011208

Tawalbeh L., Muheidat F., Tawalbeh M., and Quwaider M. (2020). IoT Privacy and Security: Challenges and Solutions. *10*, 4102. doi:10.3390/app10124102

Taylor S., and Todd P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing*, *12*(2), 137-155. doi:10.1016/0167-8116(94)00019-K

Thiagarajan D. (2016). *Analysis of the Current State of Industrial Internet of Things (IIoT) adoption. MA Thesis.* MA, USA: Massachusetts Institute of Technology, Cambridge.

Thibaud M, Chia H., Zhoua W., and Piramuthu S. (2018). Internet of Things (IoT) in high-risk Environment, Health, and Safety (EHS) industries: A comprehensive review. *Decision Support Systems, 108*, 79-95. doi:10.1016/j.dss.2018.02.005

Thompson R.L., Higgins C.A., Howell J.M. (1994). Influence of Experience on Personal Computer Utilization: Testing a Conceptual Model. *Journal of Management Information Systems, 11*(1), 167-187.

Toni M., Renzi M.F., Pasca M.G., Mugion R.G., di Pietro L., and Ungaro V. (2021). Industry 4.0 an empirical analysis of users' intention in the automotive sector. *International Journal of Quality and Service Sciences*, 22 pages. doi:10.1108/IJQSS-04-2020-0062

Trend Micro report. (2020). Industrial Internet of Things (IIoT). Retrieved from https://www.trendmicro.com/vinfo/gb/security/definition/industrial-internet-of-things-iiot%20/

Tychogiorgos G., and Bisdikian C. (2011). Selecting Relevant Sensor Providers for Meeting "Your" Quality Information Needs. *IEEE 12th International Conference on Mobile Data Management* (pp. 200-205). Lulea, Sweden: IEEE. doi:10.1109/MDM.2011.40

Vagle M.D. (2018). *Crafting Phenomenological Research* (2nd ed.). New York: Routledge. doi:10.4324/9781315173474

Venanzi R., Montori F., Bellavista P., Foschini L. (2020). Industry 4.0 Solutions for Interoperability: a Use Case about Tools and Tool Chains in the Arrowhead Tools Project. *IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 429-433). Bologna, Italy: IEEE. doi:10.1109/SMARTCOMP50058.2020.00089

Venkatesh V., and Davis F.D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh V., Davis F.D., and Morris M.G. (2008). Dead Or Alive? The Development, Trajectory, And Future Of Technology Adoption Research. *Journal of the Association for Information Systems, 8*(4). Retrieved from http://aisel.aisnet.org/jais/vol8/iss4/1

Venkatesh V., Morris M.G., Davis G.B., and Davis F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425-478. doi:10.2307/30036540

Vongsingthong S., and Smanchat S. (2014). Internet of things: a review of applications and technologies. *Suranaree Journal of Science*, 359-364.

Williams M.D., Rana N.P., and Dwivedi Y.K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of Enterprise Information Management*, *28*(3). doi:10.1108/JEIM-09-2014-0088

World Economic Forum. (2015). *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services.* World Economic Forum. Accenture. Retrieved from https://www.accenture.com/t20150527t205433__w__/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_8/accenture-industrial-internet-of-things-wef-report-2015.pdf

Xu L.D., He W. and Li S. (2014, November). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233-2243. doi:10.1109/TII.2014.2300753

Yang M., Mamun A.A., Mohiuddin M., Nawi N.C., and Zainol N.R. (2021). Cashless Transactions: A Study on Intention and Adoption of e-Wallets. *Sustainability, 2021*(13), 18 pages. doi:10.3390/su13020831

Yousafzai S.Y., Foxall G.R., and Pallister J.G. (2007). Technology acceptance: a meta-analysis of the TAM: Part 1. *Journal of Modelling in Management*, *2*(3), 1-30. doi:10.1108/17465660710834453

Zeman K. et al. (2017). Wireless M-BUS in Industrial IoT: Technology Overview and Prototype Implementation. *European Wireless 2017; 23rd European Wireless Conference* (pp. 1-6). Dresden, Germany: IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/8011289

Zhou C., Damiano N., Whisner B., and Reyes, M. (2017). Industrial Internet of Things: (IIoT) applications in underground coal mines. *Mining Engineering*, *69*(12), 50-56. doi:https://doi.org/10.19150/me.7919

Züll C. (2016). Open-Ended Questions. In *GESIS Survey Guidelines* (pp. 1-10). Mannheim, Germany: Institute for the Social Sciences. doi:10.15465/gesis-sg_en_002

APPENDICES

APPENDIX A

Systematic Literature Review on IIoT Challenges (7 Pages)

Author(s)	**Year**	**Article**	**Security**	**Interoperability**	**Integration**	**Privacy**	**Lack of Standardization**	**Heterogeneity**	**Reliability**	**IT/OT Convergence**	**Human Factors**
Ahemd et al.	2017	IoT security: A layered approach for attacks & defenses	1								
Ali et al.	2015	Internet of Things (IoT): Definitions, Challenges and Recent Research Directions	1	1	1						
Bajramovic et al.	2019	Security Challenges and Best Practices for IIoT	1	1	1			1		1	1
Bansal and Kumar	2020	IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication	1	1		1		1			
Biswas and Giaffreda	2014	IoT and cloud convergence: Opportunities and challenges		1					1		
Boye et al.	2018	Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment.	1	1	1						

Author(s)	**Year**	**Article**	**Security**	**Interoperability**	**Integration**	**Privacy**	**Lack of Standardization**	**Heterogeneity**	**Reliability**	**IT/OT Convergence**	**Human Factors**
Boyes et al.	2018	The industrial internet of things (IIoT): An analysis framework	1							1	
Chowdhury and Raut	2019	Benefits, Challenges, and Opportunities in Adoption of Industrial IoT	1	1	1		1	1			
Chowdhury et al.	2020	Identifying Barriers of Implementing IoT in Manufacturing Industry using Analytical Hierarchy Process (AHP): A Bangladeshi Perspective	1	1	1		1		1	1	
Dhirani et al.	2018	Can IoT escape Cloud QoS and Cost Pitfalls?									
Forsstrom et al.	2018	Challenges of Securing the Industrial Internet of Things Value Chain	1			1			1		
Foukalas et al.	2019	Dependable Wireless Industrial IoT Networks: Recent Advances and Open Challenges	1						1		

Author(s)	**Year**	**Article**	**Security**	**Interoperability**	**Integration**	**Privacy**	**Lack of Standardization**	**Heterogeneity**	**Reliability**	**IT/OT Convergence**	**Human Factors**
Fraile et al.	2018	Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems	1	1	1				1		
Gajek et al.	2018	IIoT and cyber-resilience	1								
Gebremichael et al.	2017	Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenge	1	1	1			1			
Gochhayat et al.	2019	Reliable and secure data transfer in IoT networks	1						1		
Gotmare and Bokade	2019	Internet of Things in Manufacturing : A Review on Applications, Challenges and Future Directions	1			1	1				1
Hameed, Khan and Hameed	2019	Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review	1		1	1					
Hassanzadeh et al.	2015	Towards effective security control assignment in the Industrial Internet of Things	1								

Author(s)	Year	Article	Security	Interoperability	Integration	Privacy	Lack of Standardization	Heterogeneity	Reliability	IT/OT Convergence	Human Factors
Hassija et al.	2019	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures	1			1			1		1
Jangid and Chauhan	2019	A Survey and Challenges in IoT Networks	1	1	1						
Karanja and et al.	2017	Internet of Things Malware : A Survey	1								
Kassab et al.	2020	A systematic literature review on Internet of things in education: Benefits and challenges	1	1							1
Khalil et al.	2021	Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications	1						1		
Khan and Khan	2019	Advanced Persistent Threats Through Industrial IoT On Oil And Gas Industry	1								
Khodadadi et al.	2017	Chapter 1 - Internet of Things: an overview	1	1	1		1		1		

Author(s)	**Year**	**Article**	**Security**	**Interoperability**	**Integration**	**Privacy**	**Lack of Standardization**	**Heterogeneity**	**Reliability**	**IT/OT Convergence**	**Human Factors**
Kim and Dang	2020	Reliability Evaluation Model Of Industrial Internet Of Things Systems							1		
Lampropoulos et al.	2019	Internet of THings in the context of Industry 4.0	1	1	1		1		1		
Lee and Lee	2015	The Internet of Things (IoT): Applications, investments, and challenges for enterprises	1			1		1			
Magomadov	2020	The Industrial Internet of Things as one of the main drivers of Industry 4.0	1								
Makrakis et al.	2021	Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures	1			1					
Moore et al.	2020	IoT reliability: a review leading to 5 key research directions	1	1					1		
Moseina and Jha	2015	A Comprehensive Study of Security of Internet-of-Things	1		1						

Author(s)	Year	Article	Security	Interoperability	Integration	Privacy	Lack of Standardization	Heterogeneity	Reliability	IT/OT Convergence	Human Factors
Nakamura and Ribeiro	2018	A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems	1			1			1		
Panchal et al.	2018	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures	1				1				
Patel and Patel	2016	Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges	1	1							
Saleem et al.	2018	IoT Standardisation - Challenges, Perspectives and Solution	1	1			1				
Sengupta et al.	2019	A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT	1			1			1		
Serpanos and Wolf	2018	Internet of Things (IoT) Systems	1		1						

Author(s)	**Year**	**Article**	**Security**	**Interoperability**	**Integration**	**Privacy**	**Lack of Standardization**	**Heterogeneity**	**Reliability**	**IT/OT Convergence**	**Human Factors**
Sisinni et al.	2018	Industrial Internet of Things: Challenges, Opportunities, and Directions	1	1	1	1	1	1			
Tange et al.	2020	A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities	1								
Tawalbeh et al.	2020	IoT Privacy and Security: Challenges and Solutions	1			1					
Thibaud et al.	2018	Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries	1	1	1			1			
Vongsingthong and Smanchat	2014	Internet of things: a review of applications and technologies	1	1	1		1		1		
			41	**19**	**16**	**11**	**9**	**7**	**15**	**3**	**4**

APPENDIX B

META-Analysis on relevant studies (1 page)

Author	Subject	Consumer or Industry Oriented	Industry Type	Research Type	Sample size	TAM	UTAUT
Kar et al.	Industrial Internet of Things and Emerging Digital Technologies–Modeling Professionals' Learning Behavior	Business	General	Survey	685		1
Toni et al.	Industry 4.0 an empirical analysis of users' intention in the automotive sector	Business	Automotive	Survey	310		
Chen et al.	THE WILLINGNESS TO ADOPT THE INTERNET OF THINGS (IoT) CONCEPTION IN TAIWAN'S CONSTRUCTION INDUSTRY	Business	Construction	Survey	282		1
Nistah et al.	Internet of Things Adoption Among Micropreneurs in Regional Coast of Sabah	Business	Agriculture	Survey	186		1
Pillai and Sivathanu	Adoption of internet of things (IoT) in the agriculture industry deploying the BRT framework	Business	Agriculture	Survey	140		1
Schrama et al.	Understanding the Knowledge Gap: How Security Awareness Influences the Adoption of Industrial IoT	Business	General	Survey	131	1	
Bakar et al.	Exploring and Developing an Industrial Automation Acceptance Model in the Manufacturing Sector Towards Adoption of Industry 4.0	Business	Manufacturing	Survey	110	1	
Goundar and Bhardwaj	Industrial Internet of Things: Benefit, Applications, and Challenges	Business	General	Survey	100	1	
Jaafreh	The Effect Factors in the Adoption of Internet of Things (IoT) Technology in the SME in KSA: An Empirical Study	Business	SMEs	Survey	72	1	
Hsu and Yeh	Understanding the factors affecting the adoption of the Internet of Things	Business	General	Survey		1	
Morienyane and Marnewick	Technology Acceptance Model of Internet of Things for Water Management at a local municipality	Business	Water Mngt	Survey	135	1	
Bautista et al.	Smart University: IoT Adoption	Business	Smart University	Survey		1	
Tsourela and Nerantzaki	An Internet of Things (IoT) Acceptance Model. Assessing Consumer's Behavior toward IoT Products and Applications	Business	General	Survey	812	1	
Isaac et al.	an empirical study of internet usage among employees in Yemen	Business	General	Survey	508	1	
Man et al.	Critical Factors Influencing Acceptance of Automated Vehicles by Hong Kong Drivers	Business	Automated Vehicles	Survey	237	1	
Park et al.	Comprehensive Approaches to User Acceptance of Internet of Things in a Smart Home Environment	Consumer	Smart Home	Survey	1057	1	
						11	**4**

APPENDIX C

Survey Findings (7 pages)

The region of the company headquartered			
		Frequency	**Percentage**
Valid answers	Turkey	255	75%
	International	87	25%
	Total	342	100%

Distribution of responses from international regions			
		Frequency	**Percentage**
Valid answers	Europe	29	33,3%
	Middle East & Africa	27	31%
	Asia	22	25,3%
	North America	6	6,9%
	South America	2	2,3%
	Total	87	100%

Sectors in which companies operate			
		Frequency	**Percentage**
Valid answers	Food	30	8.77%
	Chemical industry	25	7.31%
	Plastic and rubber production	23	6.73%
	Iron and steel industry	21	6.14%
	Paper and packaging	19	5.56%
	Pharmacy and health services	18	5.26%
	Automotive	15	4.39%
	Electronic components and equipment	14	4.09%
	Mining	14	4.09%
	Textile production	13	3.80%
	Cement production	12	3.51%
	Glass production	12	3.51%
	Retail	12	3.51%
	Technology provider	12	3.51%
	Power and renewable energy	11	3.22%
	Oil and gas	10	2.92%
	Telecommunications	10	2.92%
	Integration and contracting services	8	2.34%
	Agricultural technologies	7	2.05%
	Building automation	6	1.75%
	Logistics	5	1.46%
	Equipment provider	4	1.17%

Water technologies	4	1.17%
Aviation	3	0.88%
Construction	3	0.88%
Finance & Insurance	3	0.88%
Government	3	0.88%
Transportation	3	0.88%
Other	22	6.43%
Total	342	100%

Company ages			
		Frequency	**Percentage**
Valid answers	>10 years	210	61,4%
	5 – 10 years	104	30,4%
	3 – 5 years	26	7,6%
	Less than 3 years	2	0,6%
	Total	342	100%

Number of the employees working in the companies			
		Frequency	**Percentage**
Valid answers	Less than 100 employees	34	9,9%
	101 – 500 employees	73	21,3%
	501 – 1000 employees	83	24,3%
	1001 – 2000 employees	71	20,8%
	2001 – 5000 employees	36	10,5%
	More than 5000 employees	45	13,2%
	Total	342	100%

Technological Readiness (N=342)		
	Frequency	**Percentage**
Companies having IT and OT functions	208	60,8%
Companies having a digital transformation strategy	296	86,5%
Companies already using IIoT technologies	288	84,2%

Divisions of the participants			
		Frequency	**Percentage**
Valid answers	Information Technologies (IT)	160	46,8%
	Operational Technologies (OT)	88	25,7%
	Engineering	53	15,5%
	Others	41	12,0%
	Total	342	100%

Titles of the participants			
		Frequency	**Percentage**
Valid answers	Manager	152	44,4%
	Director	84	24,6%
	Engineer	69	20,2%
	Specialist	22	6,4%
	Others	15	4,4%
	Total	342	100%

Participants' beliefs about the most influential industry 4.0 technology in the next five years			
		Frequency	**Percentage**
Valid answers	IIoT	127	37,2%
	Advanced Robotics	115	33,6%
	Big data/Analytics	27	7,9%
	Artificial Intelligence	20	5,8%
	Blockchain	17	5,0%
	Virtual Reality	13	3,8%
	Others	23	6,7%
	Total	342	100%

Participant's experience with IIoT Technology			
		Frequency	**Percentage**
Valid answers	>10 years	15	4,4%
	5 – 10 years	94	27,5%
	3 – 5 years	150	43,9%
	1 – 3 years	69	20,1%
	Less than 1 year	14	4,1%
	Total	342	100%

Essential benefits that influence the participants to adopt IIoT (up to 3 options) (N=342)			
		Frequency	**Percentage**
Valid answers	Aumated equipment management	155	45,3%
	Eliminated human errors	127	37,1%
	Better quality and faster production	121	35,3%
	Better asset management	113	33,0%
	Improved operational efficiency	91	26,6%
	Increased equipment uptime	90	26,3%
	Reduced operating costs	87	25,4%
	More effective quality control	86	25,1%
	Improved supply chain	64	18,7%

	Enhanced facility safety/security	42	12,2%
	Increased competitiveness	19	5,5%

Challenges that affect participants to adopt IIoT (up to 3 options) (N=342)

		Frequency	**Percentage**
Valid answers	Interoperability and integration problems	189	55,2%
	Inadequacies of business partners	177	51,7%
	Security issues	164	48%
	Maintenance of the systems	151	44,1%
	Lack of qualified skills	106	31%
	Lack of standards	96	28%
	Costs	87	25,4%
	Manageability	50	14,6%

APPENDIX D

SPSS 21.0 Analysis Results (35 pages)

```
 GET
  FILE='C:\Users\Bilge\Desktop\sertan_full.sav'.
DATASET NAME DataSet1 WINDOW=FRONT.
GET DATA /TYPE=XLSX
  /FILE='C:\Users\Bilge\Downloads\SPSS_data_duzenlemesi_31102021_v2 (2).xlsx'
  /SHEET=name 'A survey study on adoption of I'
  /CELLRANGE=full
  /READNAMES=on
  /ASSUMEDSTRWIDTH=32767.
EXECUTE.
DATASET NAME DataSet2 WINDOW=FRONT.
RELIABILITY
  /VARIABLES=PT6 PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 RO
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE CORR ANOVA.
```

Reliability

Notes

Output Created		06-NOV-2021 17:16:39
Comments		
Input	Active Dataset	DataSet2
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	342
	Matrix Input	
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data for all variables in the procedure.
Syntax		RELIABILITY /VARIABLES=PT6 PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 ROI1 ROI2 PT1 PT2 PT3 PT4 PT5 PR1 PR2 PR3 PR4 PR5 FC1 FC2 FC3 BI1 BI2 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE CORR ANOVA.
Resources	Processor Time	00:00:00.02
	Elapsed Time	00:00:00.03

[DataSet2]

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	342	100.0
	Excluded[a]	0	.0
	Total	342	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.942	.942	35

Item Statistics

	Mean	Std. Deviation	N
PT6	3.52	.882	342
PU1	4.04	.631	342
PU2	4.03	.642	342
PU3	4.09	.670	342
PU4	4.11	.649	342
PEoU1	4.31	.586	342
PEoU2	4.27	.643	342
PEoU3	4.35	.623	342
PEoU4	4.38	.632	342
MO1	4.27	.705	342
MO2	4.13	.727	342
CO1	3.85	.917	342
CO2	3.23	1.033	342
CO3	3.18	1.045	342
CE1	3.61	.924	342
CE2	3.94	.686	342
CE3	4.00	.674	342
CE4	3.99	.665	342
ROI1	3.90	.767	342
ROI2	3.92	.782	342

Item Statistics

	Mean	Std. Deviation	N
PT1	3.69	.820	342
PT2	3.62	.830	342
PT3	3.49	.866	342
PT4	3.45	.887	342
PT5	3.44	.907	342
PR1	1.96	.751	342
PR2	1.84	.785	342
PR3	2.03	.790	342
PR4	1.64	.619	342
PR5	1.83	.734	342
FC1	3.95	.674	342
FC2	3.62	1.034	342
FC3	3.89	.674	342
BI1	4.17	.618	342
BI2	4.21	.592	342

Inter-Item Correlation Matrix

	PT6	PU1	PU2	PU3	PU4	PEoU1	PEoU2	PEoU3
PT6	1.000	.415	.421	.394	.386	.188	.258	.237
PU1	.415	1.000	.866	.770	.649	.399	.513	.387
PU2	.421	.866	1.000	.804	.681	.379	.498	.360
PU3	.394	.770	.804	1.000	.772	.471	.542	.377
PU4	.386	.649	.681	.772	1.000	.580	.618	.417
PEoU1	.188	.399	.379	.471	.580	1.000	.723	.615
PEoU2	.258	.513	.498	.542	.618	.723	1.000	.695
PEoU3	.237	.387	.360	.377	.417	.615	.695	1.000
PEoU4	.259	.364	.338	.366	.433	.546	.626	.867
MO1	.452	.499	.498	.511	.504	.363	.526	.561
MO2	.481	.521	.519	.493	.522	.353	.485	.469
CO1	.553	.532	.506	.506	.453	.291	.399	.358
CO2	.565	.429	.369	.397	.355	.241	.270	.253
CO3	.536	.338	.311	.320	.304	.221	.261	.250
CE1	.391	.270	.243	.258	.268	.229	.259	.291
CE2	.380	.405	.411	.415	.464	.290	.358	.307
CE3	.387	.400	.407	.436	.456	.255	.354	.303
CE4	.388	.365	.379	.391	.431	.282	.332	.310
ROI1	.410	.444	.435	.383	.423	.264	.304	.289
ROI2	.404	.440	.449	.368	.388	.224	.249	.267
PT1	.654	.446	.459	.470	.462	.190	.281	.275

Inter-Item Correlation Matrix

	PEoU4	MO1	MO2	CO1	CO2	CO3	CE1	CE2
PT6	.259	.452	.481	.553	.565	.536	.391	.380
PU1	.364	.499	.521	.532	.429	.338	.270	.405
PU2	.338	.498	.519	.506	.369	.311	.243	.411
PU3	.366	.511	.493	.506	.397	.320	.258	.415
PU4	.433	.504	.522	.453	.355	.304	.268	.464
PEoU1	.546	.363	.353	.291	.241	.221	.229	.290
PEoU2	.626	.526	.485	.399	.270	.261	.259	.358
PEoU3	.867	.561	.469	.358	.253	.250	.291	.307
PEoU4	1.000	.624	.513	.379	.249	.235	.262	.279
MO1	.624	1.000	.703	.568	.413	.380	.302	.412
MO2	.513	.703	1.000	.659	.464	.421	.367	.422
CO1	.379	.568	.659	1.000	.616	.565	.399	.445
CO2	.249	.413	.464	.616	1.000	.831	.563	.500
CO3	.235	.380	.421	.565	.831	1.000	.598	.491
CE1	.262	.302	.367	.399	.563	.598	1.000	.585
CE2	.279	.412	.422	.445	.500	.491	.585	1.000
CE3	.292	.421	.437	.474	.506	.475	.516	.824
CE4	.306	.408	.410	.448	.487	.485	.492	.749
ROI1	.277	.424	.423	.407	.473	.480	.442	.656
ROI2	.261	.409	.401	.391	.459	.449	.352	.569
PT1	.268	.487	.441	.586	.534	.534	.419	.511

Inter-Item Correlation Matrix

	CE3	CE4	ROI1	ROI2	PT1	PT2	PT3	PT4
PT6	.387	.388	.410	.404	.654	.656	.747	.790
PU1	.400	.365	.444	.440	.446	.446	.419	.381
PU2	.407	.379	.435	.449	.459	.452	.436	.366
PU3	.436	.391	.383	.368	.470	.418	.411	.373
PU4	.456	.431	.423	.388	.462	.466	.413	.382
PEoU1	.255	.282	.264	.224	.190	.203	.177	.178
PEoU2	.354	.332	.304	.249	.281	.291	.259	.228
PEoU3	.303	.310	.289	.267	.275	.240	.235	.196
PEoU4	.292	.306	.277	.261	.268	.254	.242	.211
MO1	.421	.408	.424	.409	.487	.449	.442	.395
MO2	.437	.410	.423	.401	.441	.432	.444	.392
CO1	.474	.448	.407	.391	.586	.561	.559	.525
CO2	.506	.487	.473	.459	.534	.526	.556	.563
CO3	.475	.485	.480	.449	.534	.559	.580	.578
CE1	.516	.492	.442	.352	.419	.444	.446	.409
CE2	.824	.749	.656	.569	.511	.523	.463	.404
CE3	1.000	.824	.663	.589	.529	.512	.470	.394
CE4	.824	1.000	.790	.691	.556	.532	.491	.423
ROI1	.663	.790	1.000	.885	.570	.557	.507	.445
ROI2	.589	.691	.885	1.000	.594	.569	.513	.431
PT1	.529	.556	.570	.594	1.000	.840	.784	.720

Inter-Item Correlation Matrix

	PT5	PR1	PR2	PR3	PR4	PR5	FC1	FC2
PT6	.861	-.045	.065	.014	.135	.120	.322	.348
PU1	.393	-.041	.017	.157	.040	-.025	.370	.376
PU2	.389	-.028	-.019	.137	.044	-.032	.349	.403
PU3	.366	-.034	.006	.156	.045	-.016	.349	.382
PU4	.350	-.045	-.028	.120	-.003	-.035	.335	.378
PEoU1	.156	-.100	-.095	.071	-.147	-.111	.249	.287
PEoU2	.241	-.076	-.049	.125	-.048	-.074	.263	.303
PEoU3	.216	-.109	-.075	.047	-.128	-.108	.268	.378
PEoU4	.215	-.149	-.096	.039	-.142	-.092	.267	.372
MO1	.417	-.074	-.016	.066	-.012	.048	.314	.403
MO2	.416	-.109	-.061	.050	-.028	-.026	.355	.420
CO1	.541	-.085	-.027	.074	-.015	.049	.385	.405
CO2	.549	-.068	.031	.057	.040	.066	.316	.334
CO3	.548	-.055	.039	.062	.062	.096	.301	.345
CE1	.366	-.097	-.050	.094	-.064	.004	.409	.394
CE2	.380	-.113	-.085	.068	-.123	-.027	.354	.416
CE3	.396	-.116	-.090	.077	-.108	-.025	.329	.411
CE4	.414	-.148	-.100	.034	-.120	-.053	.417	.401
ROI1	.430	-.088	-.066	.014	-.087	-.019	.392	.411
ROI2	.425	-.060	-.041	-.001	-.045	.011	.364	.344
PT1	.707	-.072	-.010	.053	.057	.079	.410	.433

Inter-Item Correlation Matrix

	FC3	BI1	BI2
PT6	.395	.366	.355
PU1	.457	.504	.467
PU2	.475	.489	.499
PU3	.425	.472	.460
PU4	.396	.501	.526
PEoU1	.196	.316	.291
PEoU2	.283	.403	.405
PEoU3	.266	.354	.344
PEoU4	.247	.361	.333
MO1	.407	.486	.465
MO2	.447	.467	.447
CO1	.433	.414	.407
CO2	.355	.343	.275
CO3	.344	.276	.242
CE1	.370	.285	.243
CE2	.448	.468	.388
CE3	.477	.466	.413
CE4	.448	.441	.440
ROI1	.421	.450	.447
ROI2	.366	.412	.426
PT1	.490	.464	.464

Inter-Item Correlation Matrix

	PT6	PU1	PU2	PU3	PU4	PEoU1	PEoU2	PEoU3
PT2	.656	.446	.452	.418	.466	.203	.291	.240
PT3	.747	.419	.436	.411	.413	.177	.259	.235
PT4	.790	.381	.366	.373	.382	.178	.228	.196
PT5	.861	.393	.389	.366	.350	.156	.241	.216
PR1	-.045	-.041	-.028	-.034	-.045	-.100	-.076	-.109
PR2	.065	.017	-.019	.006	-.028	-.095	-.049	-.075
PR3	.014	.157	.137	.156	.120	.071	.125	.047
PR4	.135	.040	.044	.045	-.003	-.147	-.048	-.128
PR5	.120	-.025	-.032	-.016	-.035	-.111	-.074	-.108
FC1	.322	.370	.349	.349	.335	.249	.263	.268
FC2	.348	.376	.403	.382	.378	.287	.303	.378
FC3	.395	.457	.475	.425	.396	.196	.283	.266
BI1	.366	.504	.489	.472	.501	.316	.403	.354
BI2	.355	.467	.499	.460	.526	.291	.405	.344

Inter-Item Correlation Matrix

	PEoU4	MO1	MO2	CO1	CO2	CO3	CE1	CE2
PT2	.254	.449	.432	.561	.526	.559	.444	.523
PT3	.242	.442	.444	.559	.556	.580	.446	.463
PT4	.211	.395	.392	.525	.563	.578	.409	.404
PT5	.215	.417	.416	.541	.549	.548	.366	.380
PR1	-.149	-.074	-.109	-.085	-.068	-.055	-.097	-.113
PR2	-.096	-.016	-.061	-.027	.031	.039	-.050	-.085
PR3	.039	.066	.050	.074	.057	.062	.094	.068
PR4	-.142	-.012	-.028	-.015	.040	.062	-.064	-.123
PR5	-.092	.048	-.026	.049	.066	.096	.004	-.027
FC1	.267	.314	.355	.385	.316	.301	.409	.354
FC2	.372	.403	.420	.405	.334	.345	.394	.416
FC3	.247	.407	.447	.433	.355	.344	.370	.448
BI1	.361	.486	.467	.414	.343	.276	.285	.468
BI2	.333	.465	.447	.407	.275	.242	.243	.388

Inter-Item Correlation Matrix

	CE3	CE4	ROI1	ROI2	PT1	PT2	PT3	PT4
PT2	.512	.532	.557	.569	.840	1.000	.840	.755
PT3	.470	.491	.507	.513	.784	.840	1.000	.834
PT4	.394	.423	.445	.431	.720	.755	.834	1.000
PT5	.396	.414	.430	.425	.707	.705	.809	.876
PR1	-.116	-.148	-.088	-.060	-.072	-.108	-.079	-.054
PR2	-.090	-.100	-.066	-.041	-.010	-.018	.014	.045
PR3	.077	.034	.014	-.001	.053	.069	.101	.063
PR4	-.108	-.120	-.087	-.045	.057	.053	.073	.105
PR5	-.025	-.053	-.019	.011	.079	.078	.070	.106
FC1	.329	.417	.392	.364	.410	.388	.411	.324
FC2	.411	.401	.411	.344	.433	.452	.414	.374
FC3	.477	.448	.421	.366	.490	.481	.434	.424
BI1	.466	.441	.450	.412	.464	.453	.380	.359
BI2	.413	.440	.447	.426	.464	.412	.389	.320

Inter-Item Correlation Matrix

	PT5	PR1	PR2	PR3	PR4	PR5	FC1	FC2
PT2	.705	-.108	-.018	.069	.053	.078	.388	.452
PT3	.809	-.079	.014	.101	.073	.070	.411	.414
PT4	.876	-.054	.045	.063	.105	.106	.324	.374
PT5	1.000	-.027	.084	.057	.140	.120	.288	.348
PR1	-.027	1.000	.711	.338	.343	.393	-.201	-.215
PR2	.084	.711	1.000	.447	.516	.569	-.254	-.195
PR3	.057	.338	.447	1.000	.379	.423	-.025	.016
PR4	.140	.343	.516	.379	1.000	.515	-.172	-.130
PR5	.120	.393	.569	.423	.515	1.000	-.350	-.192
FC1	.288	-.201	-.254	-.025	-.172	-.350	1.000	.577
FC2	.348	-.215	-.195	.016	-.130	-.192	.577	1.000
FC3	.409	-.141	-.155	.044	-.044	-.149	.555	.580
BI1	.369	-.119	-.125	.057	-.087	-.157	.521	.528
BI2	.338	-.074	-.153	.038	-.064	-.181	.513	.411

Inter-Item Correlation Matrix

	FC3	BI1	BI2
PT2	.481	.453	.412
PT3	.434	.380	.389
PT4	.424	.359	.320
PT5	.409	.369	.338
PR1	-.141	-.119	-.074
PR2	-.155	-.125	-.153
PR3	.044	.057	.038
PR4	-.044	-.087	-.064
PR5	-.149	-.157	-.181
FC1	.555	.521	.513
FC2	.580	.528	.411
FC3	1.000	.614	.521
BI1	.614	1.000	.807
BI2	.521	.807	1.000

ANOVA

		Sum of Squares	df	Mean Square	F	Sig
Between People		2364.319	341	6.933		
Within People	Between Items	7150.429	34	210.307	522.903	.000
	Residual	4662.999	11594	.402		
	Total	11813.429	11628	1.016		
Total		14177.748	11969	1.185		

Grand Mean = 3.60

```
FACTOR
 /VARIABLES PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 ROI1 R
 /MISSING LISTWISE
 /ANALYSIS PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 ROI1 RO
 /PRINT INITIAL CORRELATION KMO AIC EXTRACTION ROTATION
 /FORMAT BLANK(.4)
 /CRITERIA MINEIGEN(1) ITERATE(25)
 /EXTRACTION ML
 /CRITERIA ITERATE(25)
 /ROTATION VARIMAX.
```

Factor Analysis

Notes

Output Created		06-NOV-2021 17:18:34
Comments		
Input	Active Dataset	DataSet2
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	342
Missing Value Handling	Definition of Missing	MISSING=EXCLUDE: User-defined missing values are treated as missing.
	Cases Used	LISTWISE: Statistics are based on cases with no missing values for any variable used.
Syntax		FACTOR /VARIABLES PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 ROI1 ROI2 PT1 PT2 PT3 PT4 PT5 PT6 PR1 PR2 PR3 PR4 PR5 FC1 FC2 FC3 BI1 BI2 /MISSING LISTWISE /ANALYSIS PU1 PU2 PU3 PU4 PEoU1 PEoU2 PEoU3 PEoU4 MO1 MO2 CO1 CO2 CO3 CE1 CE2 CE3 CE4 ROI1 ROI2 PT1 PT2 PT3 PT4 PT5 PT6 PR1 PR2 PR3 PR4 PR5 FC1 FC2 FC3 BI1 BI2 /PRINT INITIAL CORRELATION KMO AIC EXTRACTION ROTATION /FORMAT BLANK(.4) /CRITERIA MINEIGEN(1) ITERATE (25) /EXTRACTION ML /CRITERIA ITERATE(25) /ROTATION VARIMAX.
Resources	Processor Time	00:00:00.06
	Elapsed Time	00:00:00.06
	Maximum Memory Required	141888 (138.563K) bytes

[DataSet2]

Correlation Matrix

		PU1	PU2	PU3	PU4	PEoU1	PEoU2	PEoU3
Correlation	PU1	1.000	.866	.770	.649	.399	.513	.387
	PU2	.866	1.000	.804	.681	.379	.498	.360
	PU3	.770	.804	1.000	.772	.471	.542	.377
	PU4	.649	.681	.772	1.000	.580	.618	.417
	PEoU1	.399	.379	.471	.580	1.000	.723	.615
	PEoU2	.513	.498	.542	.618	.723	1.000	.695
	PEoU3	.387	.360	.377	.417	.615	.695	1.000
	PEoU4	.364	.338	.366	.433	.546	.626	.867
	MO1	.499	.498	.511	.504	.363	.526	.561
	MO2	.521	.519	.493	.522	.353	.485	.469
	CO1	.532	.506	.506	.453	.291	.399	.358
	CO2	.429	.369	.397	.355	.241	.270	.253
	CO3	.338	.311	.320	.304	.221	.261	.250
	CE1	.270	.243	.258	.268	.229	.259	.291
	CE2	.405	.411	.415	.464	.290	.358	.307
	CE3	.400	.407	.436	.456	.255	.354	.303
	CE4	.365	.379	.391	.431	.282	.332	.310
	ROI1	.444	.435	.383	.423	.264	.304	.289
	ROI2	.440	.449	.368	.388	.224	.249	.267
	PT1	.446	.459	.470	.462	.190	.281	.275
	PT2	.446	.452	.418	.466	.203	.291	.240
	PT3	.419	.436	.411	.413	.177	.259	.235
	PT4	.381	.366	.373	.382	.178	.228	.196
	PT5	.393	.389	.366	.350	.156	.241	.216
	PT6	.415	.421	.394	.386	.188	.258	.237
	PR1	-.041	-.028	-.034	-.045	-.100	-.076	-.109
	PR2	.017	-.019	.006	-.028	-.095	-.049	-.075
	PR3	.157	.137	.156	.120	.071	.125	.047
	PR4	.040	.044	.045	-.003	-.147	-.048	-.128
	PR5	-.025	-.032	-.016	-.035	-.111	-.074	-.108
	FC1	.370	.349	.349	.335	.249	.263	.268
	FC2	.376	.403	.382	.378	.287	.303	.378
	FC3	.457	.475	.425	.396	.196	.283	.266
	BI1	.504	.489	.472	.501	.316	.403	.354
	BI2	.467	.499	.460	.526	.291	.405	.344

Correlation Matrix

		PEoU4	MO1	MO2	CO1	CO2	CO3	CE1
Correlation	PU1	.364	.499	.521	.532	.429	.338	.270
	PU2	.338	.498	.519	.506	.369	.311	.243
	PU3	.366	.511	.493	.506	.397	.320	.258
	PU4	.433	.504	.522	.453	.355	.304	.268
	PEoU1	.546	.363	.353	.291	.241	.221	.229
	PEoU2	.626	.526	.485	.399	.270	.261	.259
	PEoU3	.867	.561	.469	.358	.253	.250	.291
	PEoU4	1.000	.624	.513	.379	.249	.235	.262
	MO1	.624	1.000	.703	.568	.413	.380	.302
	MO2	.513	.703	1.000	.659	.464	.421	.367
	CO1	.379	.568	.659	1.000	.616	.565	.399
	CO2	.249	.413	.464	.616	1.000	.831	.563
	CO3	.235	.380	.421	.565	.831	1.000	.598
	CE1	.262	.302	.367	.399	.563	.598	1.000
	CE2	.279	.412	.422	.445	.500	.491	.585
	CE3	.292	.421	.437	.474	.506	.475	.516
	CE4	.306	.408	.410	.448	.487	.485	.492
	ROI1	.277	.424	.423	.407	.473	.480	.442
	ROI2	.261	.409	.401	.391	.459	.449	.352
	PT1	.268	.487	.441	.586	.534	.534	.419
	PT2	.254	.449	.432	.561	.526	.559	.444
	PT3	.242	.442	.444	.559	.556	.580	.446
	PT4	.211	.395	.392	.525	.563	.578	.409
	PT5	.215	.417	.416	.541	.549	.548	.366
	PT6	.259	.452	.481	.553	.565	.536	.391
	PR1	-.149	-.074	-.109	-.085	-.068	-.055	-.097
	PR2	-.096	-.016	-.061	-.027	.031	.039	-.050
	PR3	.039	.066	.050	.074	.057	.062	.094
	PR4	-.142	-.012	-.028	-.015	.040	.062	-.064
	PR5	-.092	.048	-.026	.049	.066	.096	.004
	FC1	.267	.314	.355	.385	.316	.301	.409
	FC2	.372	.403	.420	.405	.334	.345	.394
	FC3	.247	.407	.447	.433	.355	.344	.370
	BI1	.361	.486	.467	.414	.343	.276	.285
	BI2	.333	.465	.447	.407	.275	.242	.243

Correlation Matrix

		CE2	CE3	CE4	ROI1	ROI2	PT1	PT2
Correlation	PU1	.405	.400	.365	.444	.440	.446	.446
	PU2	.411	.407	.379	.435	.449	.459	.452
	PU3	.415	.436	.391	.383	.368	.470	.418
	PU4	.464	.456	.431	.423	.388	.462	.466
	PEoU1	.290	.255	.282	.264	.224	.190	.203
	PEoU2	.358	.354	.332	.304	.249	.281	.291
	PEoU3	.307	.303	.310	.289	.267	.275	.240
	PEoU4	.279	.292	.306	.277	.261	.268	.254
	MO1	.412	.421	.408	.424	.409	.487	.449
	MO2	.422	.437	.410	.423	.401	.441	.432
	CO1	.445	.474	.448	.407	.391	.586	.561
	CO2	.500	.506	.487	.473	.459	.534	.526
	CO3	.491	.475	.485	.480	.449	.534	.559
	CE1	.585	.516	.492	.442	.352	.419	.444
	CE2	1.000	.824	.749	.656	.569	.511	.523
	CE3	.824	1.000	.824	.663	.589	.529	.512
	CE4	.749	.824	1.000	.790	.691	.556	.532
	ROI1	.656	.663	.790	1.000	.885	.570	.557
	ROI2	.569	.589	.691	.885	1.000	.594	.569
	PT1	.511	.529	.556	.570	.594	1.000	.840
	PT2	.523	.512	.532	.557	.569	.840	1.000
	PT3	.463	.470	.491	.507	.513	.784	.840
	PT4	.404	.394	.423	.445	.431	.720	.755
	PT5	.380	.396	.414	.430	.425	.707	.705
	PT6	.380	.387	.388	.410	.404	.654	.656
	PR1	-.113	-.116	-.148	-.088	-.060	-.072	-.108
	PR2	-.085	-.090	-.100	-.066	-.041	-.010	-.018
	PR3	.068	.077	.034	.014	-.001	.053	.069
	PR4	-.123	-.108	-.120	-.087	-.045	.057	.053
	PR5	-.027	-.025	-.053	-.019	.011	.079	.078
	FC1	.354	.329	.417	.392	.364	.410	.388
	FC2	.416	.411	.401	.411	.344	.433	.452
	FC3	.448	.477	.448	.421	.366	.490	.481
	BI1	.468	.466	.441	.450	.412	.464	.453
	BI2	.388	.413	.440	.447	.426	.464	.412

Correlation Matrix

		PT3	PT4	PT5	PT6	PR1	PR2	PR3
Correlation	PU1	.419	.381	.393	.415	-.041	.017	.157
	PU2	.436	.366	.389	.421	-.028	-.019	.137
	PU3	.411	.373	.366	.394	-.034	.006	.156
	PU4	.413	.382	.350	.386	-.045	-.028	.120
	PEoU1	.177	.178	.156	.188	-.100	-.095	.071
	PEoU2	.259	.228	.241	.258	-.076	-.049	.125
	PEoU3	.235	.196	.216	.237	-.109	-.075	.047
	PEoU4	.242	.211	.215	.259	-.149	-.096	.039
	MO1	.442	.395	.417	.452	-.074	-.016	.066
	MO2	.444	.392	.416	.481	-.109	-.061	.050
	CO1	.559	.525	.541	.553	-.085	-.027	.074
	CO2	.556	.563	.549	.565	-.068	.031	.057
	CO3	.580	.578	.548	.536	-.055	.039	.062
	CE1	.446	.409	.366	.391	-.097	-.050	.094
	CE2	.463	.404	.380	.380	-.113	-.085	.068
	CE3	.470	.394	.396	.387	-.116	-.090	.077
	CE4	.491	.423	.414	.388	-.148	-.100	.034
	ROI1	.507	.445	.430	.410	-.088	-.066	.014
	ROI2	.513	.431	.425	.404	-.060	-.041	-.001
	PT1	.784	.720	.707	.654	-.072	-.010	.053
	PT2	.840	.755	.705	.656	-.108	-.018	.069
	PT3	1.000	.834	.809	.747	-.079	.014	.101
	PT4	.834	1.000	.876	.790	-.054	.045	.063
	PT5	.809	.876	1.000	.861	-.027	.084	.057
	PT6	.747	.790	.861	1.000	-.045	.065	.014
	PR1	-.079	-.054	-.027	-.045	1.000	.711	.338
	PR2	.014	.045	.084	.065	.711	1.000	.447
	PR3	.101	.063	.057	.014	.338	.447	1.000
	PR4	.073	.105	.140	.135	.343	.516	.379
	PR5	.070	.106	.120	.120	.393	.569	.423
	FC1	.411	.324	.288	.322	-.201	-.254	-.025
	FC2	.414	.374	.348	.348	-.215	-.195	.016
	FC3	.434	.424	.409	.395	-.141	-.155	.044
	BI1	.380	.359	.369	.366	-.119	-.125	.057
	BI2	.389	.320	.338	.355	-.074	-.153	.038

Correlation Matrix

		PR4	PR5	FC1	FC2	FC3	BI1	BI2
Correlation	PU1	.040	-.025	.370	.376	.457	.504	.467
	PU2	.044	-.032	.349	.403	.475	.489	.499
	PU3	.045	-.016	.349	.382	.425	.472	.460
	PU4	-.003	-.035	.335	.378	.396	.501	.526
	PEoU1	-.147	-.111	.249	.287	.196	.316	.291
	PEoU2	-.048	-.074	.263	.303	.283	.403	.405
	PEoU3	-.128	-.108	.268	.378	.266	.354	.344
	PEoU4	-.142	-.092	.267	.372	.247	.361	.333
	MO1	-.012	.048	.314	.403	.407	.486	.465
	MO2	-.028	-.026	.355	.420	.447	.467	.447
	CO1	-.015	.049	.385	.405	.433	.414	.407
	CO2	.040	.066	.316	.334	.355	.343	.275
	CO3	.062	.096	.301	.345	.344	.276	.242
	CE1	-.064	.004	.409	.394	.370	.285	.243
	CE2	-.123	-.027	.354	.416	.448	.468	.388
	CE3	-.108	-.025	.329	.411	.477	.466	.413
	CE4	-.120	-.053	.417	.401	.448	.441	.440
	ROI1	-.087	-.019	.392	.411	.421	.450	.447
	ROI2	-.045	.011	.364	.344	.366	.412	.426
	PT1	.057	.079	.410	.433	.490	.464	.464
	PT2	.053	.078	.388	.452	.481	.453	.412
	PT3	.073	.070	.411	.414	.434	.380	.389
	PT4	.105	.106	.324	.374	.424	.359	.320
	PT5	.140	.120	.288	.348	.409	.369	.338
	PT6	.135	.120	.322	.348	.395	.366	.355
	PR1	.343	.393	-.201	-.215	-.141	-.119	-.074
	PR2	.516	.569	-.254	-.195	-.155	-.125	-.153
	PR3	.379	.423	-.025	.016	.044	.057	.038
	PR4	1.000	.515	-.172	-.130	-.044	-.087	-.064
	PR5	.515	1.000	-.350	-.192	-.149	-.157	-.181
	FC1	-.172	-.350	1.000	.577	.555	.521	.513
	FC2	-.130	-.192	.577	1.000	.580	.528	.411
	FC3	-.044	-.149	.555	.580	1.000	.614	.521
	BI1	-.087	-.157	.521	.528	.614	1.000	.807
	BI2	-.064	-.181	.513	.411	.521	.807	1.000

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.920
Bartlett's Test of Sphericity	Approx. Chi-Square	10411.807
	df	595
	Sig.	.000

Anti-image Matrices

		PU1	PU2	PU3	PU4	PEoU1	PEoU2
Anti-image Covariance	PU1	.200	-.113	-.034	.000	.005	-.012
	PU2	-.113	.175	-.068	-.014	.018	-.009

Anti-image Matrices

		PEoU3	PEoU4	MO1	MO2	CO1	CO2
Anti-image Covariance	PU1	-.010	.002	.004	-.003	-.025	-.030
	PU2	-.001	.008	.000	-.008	-.004	.019

Anti-image Matrices

		CO3	CE1	CE2	CE3	CE4	ROI1
Anti-image Covariance	PU1	.018	.002	.003	-.003	.025	-.020
	PU2	-.006	.006	-.012	.015	-.006	.013

Anti-image Matrices

		ROI2	PT1	PT2	PT3	PT4	PT5
Anti-image Covariance	PU1	.002	.011	-.010	.012	-.006	-.004
	PU2	-.026	.012	-.003	-.014	.018	-.001

Anti-image Matrices

		PT6	PR1	PR2	PR3	PR4	PR5
Anti-image Covariance	PU1	.007	.027	-.026	-.020	.004	.009
	PU2	-.017	-.025	.023	-.004	-.007	.004

Anti-image Matrices

		FC1	FC2	FC3	BI1	BI2
Anti-image Covariance	PU1	-.029	.034	-.003	-.023	.019
	PU2	.034	-.033	-.031	.017	-.022

Anti-image Matrices

		PU1	PU2	PU3	PU4	PEoU1	PEoU2
	PU3	-.034	-.068	.224	-.098	-.022	-.001
	PU4	.000	-.014	-.098	.267	-.085	-.038
	PEoU1	.005	.018	-.022	-.085	.368	-.135
	PEoU2	-.012	-.009	-.001	-.038	-.135	.296
	PEoU3	-.010	-.001	.003	.038	-.053	-.064
	PEoU4	.002	.008	.008	-.029	.007	.004
	MO1	.004	.000	-.030	.014	.037	-.030
	MO2	-.003	-.008	.022	-.044	.014	-.013
	CO1	-.025	-.004	-.015	.032	-.004	-.010
	CO2	-.030	.019	-.011	-.003	-.011	.018
	CO3	.018	-.006	.005	.011	-.006	-.014
	CE1	.002	.006	.004	.020	-.003	.003
	CE2	.003	-.012	.012	-.025	-.002	-.003
	CE3	-.003	.015	-.019	-.006	.031	-.019
	CE4	.025	-.006	-.004	.001	-.016	.007
	ROI1	-.020	.013	.005	-.005	.002	-.011
	ROI2	.002	-.026	.012	.012	-.014	.028
	PT1	.011	.012	-.035	-.003	.020	.014
	PT2	-.010	-.003	.030	-.029	.005	-.016
	PT3	.012	-.014	-.003	.007	.007	.007
	PT4	-.006	.018	-.008	-.016	-.011	.007
	PT5	-.004	-.001	.006	.013	.007	-.012
	PT6	.007	-.017	.004	-.002	-.012	.012
	PR1	.027	-.025	.009	-.010	-.005	.006
	PR2	-.026	.023	-.009	-.005	.016	.002
	PR3	-.020	-.004	-.008	.013	-.024	-.020
	PR4	.004	-.007	-.014	-.006	.054	-.032
	PR5	.009	.004	.005	-.004	-.008	.015
	FC1	-.029	.034	-.015	.010	-.012	-.004
	FC2	.034	-.033	-.005	-.005	-.014	.042
	FC3	-.003	-.031	.007	.013	.019	.012
	BI1	-.023	.017	-.007	.017	-.018	.000
	BI2	.019	-.022	.019	-.052	.030	-.015
Anti-image Correlation	PU1	.924[a]	-.603	-.160	-.002	.018	-.050
	PU2	-.603	.909[a]	-.344	-.064	.072	-.041
	PU3	-.160	-.344	.939[a]	-.400	-.077	-.005
	PU4	-.002	-.064	-.400	.938[a]	-.272	-.134
	PEoU1	.018	.072	-.077	-.272	.904[a]	-.407
	PEoU2	-.050	-.041	-.005	-.134	-.407	.935[a]

Anti-image Matrices

		PEoU3	PEoU4	MO1	MO2	CO1	CO2
	PU3	.003	.008	-.030	.022	-.015	-.011
	PU4	.038	-.029	.014	-.044	.032	-.003
	PEoU1	-.053	.007	.037	.014	-.004	-.011
	PEoU2	-.064	.004	-.030	-.013	-.010	.018
	PEoU3	.186	-.139	.002	.004	.008	.003
	PEoU4	-.139	.203	-.070	-.015	-.008	.004
	MO1	.002	-.070	.345	-.126	-.014	-.005
	MO2	.004	-.015	-.126	.354	-.122	.001
	CO1	.008	-.008	-.014	-.122	.356	-.056
	CO2	.003	.004	-.005	.001	-.056	.240
	CO3	-.003	.004	-.001	-3.953E-005	-.020	-.158
	CE1	-.021	-.002	.029	-.033	.036	-.038
	CE2	-.011	.021	-.015	.006	.001	.004
	CE3	.002	.000	.006	-.002	-.015	-.015
	CE4	.004	-.013	.006	.007	-.008	-.001
	ROI1	.004	.008	-.008	-.003	.010	.012
	ROI2	-.006	-.007	.001	-.013	.022	-.020
	PT1	-.021	.014	-.021	.024	-.034	-.006
	PT2	.014	-.005	.003	.016	-.020	.020
	PT3	-.004	.003	-.005	-.014	.010	.001
	PT4	.010	-.008	.004	.012	.003	-.006
	PT5	-.009	.011	-.001	.009	-.014	.004
	PT6	.010	-.014	-.003	-.035	.003	-.026
	PR1	-.009	.020	-.003	.008	-.006	.008
	PR2	-.010	.000	-.002	.002	.007	-.006
	PR3	.014	-.018	.024	.001	-.001	.002
	PR4	-.003	.022	.009	-.015	.047	-.005
	PR5	.014	-.002	-.050	.023	-.046	.018
	FC1	.016	-.004	.009	.019	-.041	.007
	FC2	-.030	-.010	-.004	-.012	-.007	.018
	FC3	-.013	.024	-.008	-.036	.007	.015
	BI1	.015	-.016	-.013	-.009	.029	-.032
	BI2	-.017	.017	-.015	.006	-.025	.026
Anti-image Correlation	PU1	-.050	.010	.017	-.012	-.093	-.136
	PU2	-.006	.041	.001	-.031	-.017	.094
	PU3	.016	.037	-.107	.078	-.052	-.049
	PU4	.172	-.126	.046	-.143	.102	-.011
	PEoU1	-.201	.026	.104	.040	-.010	-.036
	PEoU2	-.272	.018	-.093	-.042	-.030	.067

Anti-image Matrices

		CO3	CE1	CE2	CE3	CE4	ROI1
	PU3	.005	.004	.012	-.019	-.004	.005
	PU4	.011	.020	-.025	-.006	.001	-.005
	PEoU1	-.006	-.003	-.002	.031	-.016	.002
	PEoU2	-.014	.003	-.003	-.019	.007	-.011
	PEoU3	-.003	-.021	-.011	.002	.004	.004
	PEoU4	.004	-.002	.021	.000	-.013	.008
	MO1	-.001	.029	-.015	.006	.006	-.008
	MO2	-3.953E-005	-.033	.006	-.002	.007	-.003
	CO1	-.020	.036	.001	-.015	-.008	.010
	CO2	-.158	-.038	.004	-.015	-.001	.012
	CO3	.251	-.066	-.004	.009	-.004	-.010
	CE1	-.066	.451	-.087	-.013	.011	-.023
	CE2	-.004	-.087	.253	-.103	-.021	-.016
	CE3	.009	-.013	-.103	.198	-.096	.017
	CE4	-.004	.011	-.021	-.096	.191	-.064
	ROI1	-.010	-.023	-.016	.017	-.064	.141
	ROI2	.001	.041	.005	-.014	.011	-.116
	PT1	.010	-.001	.003	-.003	-.008	.008
	PT2	-.017	-.012	-.012	.007	-.001	.005
	PT3	-.008	-.003	.003	-.012	.006	.001
	PT4	-.013	-.005	-.004	.016	-.001	-.006
	PT5	-.003	.014	.008	.000	-.010	.001
	PT6	.014	-.016	-.002	-.008	.015	-.004
	PR1	-.002	.001	-.003	-.015	.035	-.008
	PR2	-.003	.004	.001	.017	-.021	.003
	PR3	.015	-.038	-.001	-.021	.001	.001
	PR4	-.022	.026	.022	.011	.003	.014
	PR5	-.010	-.035	-.001	.004	.000	-.001
	FC1	.008	-.091	.006	.058	-.050	.019
	FC2	-.018	-.017	.003	-.020	.027	-.032
	FC3	-.009	-.011	.011	-.037	-.002	-.006
	BI1	.024	.031	-.036	-.011	.022	-.002
	BI2	-.009	-.006	.031	.006	-.021	-.004
Anti-image Correlation	PU1	.082	.006	.014	-.017	.127	-.121
	PU2	-.030	.020	-.055	.079	-.031	.084
	PU3	.019	.014	.051	-.089	-.021	.031
	PU4	.043	.058	-.095	-.027	.005	-.026
	PEoU1	-.019	-.006	-.007	.116	-.062	.008
	PEoU2	-.050	.009	-.010	-.077	.028	-.056

Anti-image Matrices

		ROI2	PT1	PT2	PT3	PT4	PT5
	PU3	.012	-.035	.030	-.003	-.008	.006
	PU4	.012	-.003	-.029	.007	-.016	.013
	PEoU1	-.014	.020	.005	.007	-.011	.007
	PEoU2	.028	.014	-.016	.007	.007	-.012
	PEoU3	-.006	-.021	.014	-.004	.010	-.009
	PEoU4	-.007	.014	-.005	.003	-.008	.011
	MO1	.001	-.021	.003	-.005	.004	-.001
	MO2	-.013	.024	.016	-.014	.012	.009
	CO1	.022	-.034	-.020	.010	.003	-.014
	CO2	-.020	-.006	.020	.001	-.006	.004
	CO3	.001	.010	-.017	-.008	-.013	-.003
	CE1	.041	-.001	-.012	-.003	-.005	.014
	CE2	.005	.003	-.012	.003	-.004	.008
	CE3	-.014	-.003	.007	-.012	.016	.000
	CE4	.011	-.008	-.001	.006	-.001	-.010
	ROI1	-.116	.008	.005	.001	-.006	.001
	ROI2	.179	-.028	-.016	-.002	.008	-.001
	PT1	-.028	.216	-.087	-.015	-.005	-.018
	PT2	-.016	-.087	.178	-.070	-.020	.015
	PT3	-.002	-.015	-.070	.164	-.042	-.029
	PT4	.008	-.005	-.020	-.042	.167	-.070
	PT5	-.001	-.018	.015	-.029	-.070	.138
	PT6	.010	.002	-.001	-.009	-.014	-.089
	PR1	-.005	-.010	.015	.010	-.007	-.002
	PR2	1.606E-005	.008	.000	-.005	.009	-.008
	PR3	.022	.017	.008	-.043	.000	-.002
	PR4	-.009	-.005	-.008	.014	.003	-.011
	PR5	-.015	-.020	-.008	.010	-.005	.015
	FC1	-.030	-.011	.025	-.046	.008	.032
	FC2	.030	.002	-.023	.005	-.005	-.004
	FC3	.025	-.016	-.014	.026	-.023	-.008
	BI1	.005	.008	-.028	.031	-.004	-.016
	BI2	-.007	-.023	.025	-.021	.012	.008
Anti-image Correlation	PU1	.010	.053	-.054	.066	-.035	-.026
	PU2	-.149	.062	-.015	-.084	.107	-.004
	PU3	.060	-.160	.151	-.017	-.040	.034
	PU4	.056	-.014	-.134	.033	-.077	.069
	PEoU1	-.054	.072	.020	.030	-.045	.033
	PEoU2	.121	.056	-.071	.031	.034	-.060

Anti-image Matrices

		PT6	PR1	PR2	PR3	PR4	PR5
	PU3	.004	.009	-.009	-.008	-.014	.005
	PU4	-.002	-.010	-.005	.013	-.006	-.004
	PEoU1	-.012	-.005	.016	-.024	.054	-.008
	PEoU2	.012	.006	.002	-.020	-.032	.015
	PEoU3	.010	-.009	-.010	.014	-.003	.014
	PEoU4	-.014	.020	.000	-.018	.022	-.002
	MO1	-.003	-.003	-.002	.024	.009	-.050
	MO2	-.035	.008	.002	.001	-.015	.023
	CO1	.003	-.006	.007	-.001	.047	-.046
	CO2	-.026	.008	-.006	.002	-.005	.018
	CO3	.014	-.002	-.003	.015	-.022	-.010
	CE1	-.016	.001	.004	-.038	.026	-.035
	CE2	-.002	-.003	.001	-.001	.022	-.001
	CE3	-.008	-.015	.017	-.021	.011	.004
	CE4	.015	.035	-.021	.001	.003	.000
	ROI1	-.004	-.008	.003	.001	.014	-.001
	ROI2	.010	-.005	1.606E-005	.022	-.009	-.015
	PT1	.002	-.010	.008	.017	-.005	-.020
	PT2	-.001	.015	.000	.008	-.008	-.008
	PT3	-.009	.010	-.005	-.043	.014	.010
	PT4	-.014	-.007	.009	.000	.003	-.005
	PT5	-.089	-.002	-.008	-.002	-.011	.015
	PT6	.215	.012	-.012	.061	-.022	-.031
	PR1	.012	.450	-.241	-.028	.030	-.005
	PR2	-.012	-.241	.333	-.075	-.099	-.085
	PR3	.061	-.028	-.075	.637	-.097	-.135
	PR4	-.022	.030	-.099	-.097	.579	-.137
	PR5	-.031	-.005	-.085	-.135	-.137	.474
	FC1	-.030	-.020	.019	-.031	-.011	.119
	FC2	.009	.031	.001	-.017	.003	.012
	FC3	.010	-.010	.023	-.009	-.030	.009
	BI1	.012	.025	-.027	-.007	.023	-.007
	BI2	-.017	-.045	.042	-.011	-.027	.028
Anti-image Correlation	PU1	.033	.090	-.102	-.056	.012	.029
	PU2	-.085	-.089	.097	-.013	-.021	.015
	PU3	.017	.030	-.032	-.021	-.039	.015
	PU4	-.010	-.028	-.016	.031	-.015	-.011
	PEoU1	-.044	-.013	.046	-.049	.117	-.020
	PEoU2	.049	.015	.005	-.047	-.078	.040

Anti-image Matrices

		FC1	FC2	FC3	BI1	BI2
	PU3	-.015	-.005	.007	-.007	.019
	PU4	.010	-.005	.013	.017	-.052
	PEoU1	-.012	-.014	.019	-.018	.030
	PEoU2	-.004	.042	.012	.000	-.015
	PEoU3	.016	-.030	-.013	.015	-.017
	PEoU4	-.004	-.010	.024	-.016	.017
	MO1	.009	-.004	-.008	-.013	-.015
	MO2	.019	-.012	-.036	-.009	.006
	CO1	-.041	-.007	.007	.029	-.025
	CO2	.007	.018	.015	-.032	.026
	CO3	.008	-.018	-.009	.024	-.009
	CE1	-.091	-.017	-.011	.031	-.006
	CE2	.006	.003	.011	-.036	.031
	CE3	.058	-.020	-.037	-.011	.006
	CE4	-.050	.027	-.002	.022	-.021
	ROI1	.019	-.032	-.006	-.002	-.004
	ROI2	-.030	.030	.025	.005	-.007
	PT1	-.011	.002	-.016	.008	-.023
	PT2	.025	-.023	-.014	-.028	.025
	PT3	-.046	.005	.026	.031	-.021
	PT4	.008	-.005	-.023	-.004	.012
	PT5	.032	-.004	-.008	-.016	.008
	PT6	-.030	.009	.010	.012	-.017
	PR1	-.020	.031	-.010	.025	-.045
	PR2	.019	.001	.023	-.027	.042
	PR3	-.031	-.017	-.009	-.007	-.011
	PR4	-.011	.003	-.030	.023	-.027
	PR5	.119	.012	.009	-.007	.028
	FC1	.406	-.121	-.085	-.019	-.036
	FC2	-.121	.465	-.083	-.058	.051
	FC3	-.085	-.083	.430	-.067	.008
	BI1	-.019	-.058	-.067	.241	-.170
	BI2	-.036	.051	.008	-.170	.264
Anti-image Correlation	PU1	-.103	.112	-.012	-.107	.080
	PU2	.126	-.115	-.113	.084	-.103
	PU3	-.050	-.014	.021	-.030	.077
	PU4	.029	-.015	.037	.066	-.194
	PEoU1	-.030	-.034	.048	-.061	.097
	PEoU2	-.010	.113	.032	.001	-.052

Anti-image Matrices

	PU1	PU2	PU3	PU4	PEoU1	PEoU2
PEoU3	-.050	-.006	.016	.172	-.201	-.272
PEoU4	.010	.041	.037	-.126	.026	.018
MO1	.017	.001	-.107	.046	.104	-.093
MO2	-.012	-.031	.078	-.143	.040	-.042
CO1	-.093	-.017	-.052	.102	-.010	-.030
CO2	-.136	.094	-.049	-.011	-.036	.067
CO3	.082	-.030	.019	.043	-.019	-.050
CE1	.006	.020	.014	.058	-.006	.009
CE2	.014	-.055	.051	-.095	-.007	-.010
CE3	-.017	.079	-.089	-.027	.116	-.077
CE4	.127	-.031	-.021	.005	-.062	.028
ROI1	-.121	.084	.031	-.026	.008	-.056
ROI2	.010	-.149	.060	.056	-.054	.121
PT1	.053	.062	-.160	-.014	.072	.056
PT2	-.054	-.015	.151	-.134	.020	-.071
PT3	.066	-.084	-.017	.033	.030	.031
PT4	-.035	.107	-.040	-.077	-.045	.034
PT5	-.026	-.004	.034	.069	.033	-.060
PT6	.033	-.085	.017	-.010	-.044	.049
PR1	.090	-.089	.030	-.028	-.013	.015
PR2	-.102	.097	-.032	-.016	.046	.005
PR3	-.056	-.013	-.021	.031	-.049	-.047
PR4	.012	-.021	-.039	-.015	.117	-.078
PR5	.029	.015	.015	-.011	-.020	.040
FC1	-.103	.126	-.050	.029	-.030	-.010
FC2	.112	-.115	-.014	-.015	-.034	.113
FC3	-.012	-.113	.021	.037	.048	.032
BI1	-.107	.084	-.030	.066	-.061	.001
BI2	.080	-.103	.077	-.194	.097	-.052

Anti-image Matrices

	PEoU3	PEoU4	MO1	MO2	CO1	CO2
PEoU3	.858[a]	-.718	.006	.016	.032	.015
PEoU4	-.718	.865[a]	-.267	-.055	-.028	.017
MO1	.006	-.267	.958[a]	-.360	-.040	-.017
MO2	.016	-.055	-.360	.948[a]	-.344	.002
CO1	.032	-.028	-.040	-.344	.959[a]	-.191
CO2	.015	.017	-.017	.002	-.191	.914[a]
CO3	-.015	.019	-.003	.000	-.069	-.642
CE1	-.072	-.007	.075	-.083	.090	-.116
CE2	-.049	.093	-.050	.020	.002	.015
CE3	.011	.001	.021	-.009	-.056	-.069
CE4	.019	-.067	.022	.029	-.030	-.006
ROI1	.024	.047	-.036	-.014	.047	.064
ROI2	-.031	-.037	.003	-.053	.087	-.096
PT1	-.106	.066	-.077	.085	-.123	-.025
PT2	.080	-.028	.013	.065	-.078	.098
PT3	-.024	.015	-.022	-.058	.040	.003
PT4	.057	-.043	.015	.050	.014	-.029
PT5	-.055	.067	-.005	.042	-.063	.021
PT6	.049	-.068	-.011	-.127	.010	-.116
PR1	-.032	.067	-.007	.019	-.015	.023
PR2	-.040	.001	-.005	.005	.020	-.022
PR3	.041	-.049	.051	.001	-.002	.006
PR4	-.009	.063	.019	-.033	.103	-.014
PR5	.048	-.008	-.124	.055	-.111	.054
FC1	.059	-.015	.023	.049	-.109	.022
FC2	-.101	-.034	-.010	-.028	-.017	.053
FC3	-.046	.081	-.022	-.093	.019	.048
BI1	.070	-.071	-.045	-.032	.098	-.132
BI2	-.078	.073	-.049	.019	-.081	.105

Anti-image Matrices

	CO3	CE1	CE2	CE3	CE4	ROI1
PEoU3	-.015	-.072	-.049	.011	.019	.024
PEoU4	.019	-.007	.093	.001	-.067	.047
MO1	-.003	.075	-.050	.021	.022	-.036
MO2	.000	-.083	.020	-.009	.029	-.014
CO1	-.069	.090	.002	-.056	-.030	.047
CO2	-.642	-.116	.015	-.069	-.006	.064
CO3	.919[a]	-.197	-.018	.042	-.020	-.052
CE1	-.197	.945[a]	-.258	-.042	.037	-.092
CE2	-.018	-.258	.947[a]	-.460	-.098	-.084
CE3	.042	-.042	-.460	.917[a]	-.492	.099
CE4	-.020	.037	-.098	-.492	.928[a]	-.392
ROI1	-.052	-.092	-.084	.099	-.392	.898[a]
ROI2	.007	.146	.024	-.076	.061	-.729
PT1	.044	-.002	.013	-.014	-.041	.046
PT2	-.080	-.041	-.058	.037	-.007	.029
PT3	-.040	-.010	.016	-.065	.031	.006
PT4	-.064	-.020	-.019	.089	-.007	-.039
PT5	-.016	.056	.042	.003	-.061	.009
PT6	.058	-.050	-.007	-.039	.074	-.023
PR1	-.006	.002	-.010	-.050	.119	-.033
PR2	-.011	.010	.004	.065	-.084	.012
PR3	.038	-.071	-.002	-.058	.002	.002
PR4	-.057	.050	.057	.031	.009	.048
PR5	-.029	-.075	-.004	.014	-.001	-.003
FC1	.026	-.214	.020	.204	-.178	.078
FC2	-.053	-.037	.008	-.065	.090	-.126
FC3	-.026	-.025	.034	-.127	-.007	-.025
BI1	.097	.093	-.146	-.050	.102	-.011
BI2	-.037	-.017	.118	.024	-.096	-.020

Anti-image Matrices

	ROI2	PT1	PT2	PT3	PT4	PT5
PEoU3	-.031	-.106	.080	-.024	.057	-.055
PEoU4	-.037	.066	-.028	.015	-.043	.067
MO1	.003	-.077	.013	-.022	.015	-.005
MO2	-.053	.085	.065	-.058	.050	.042
CO1	.087	-.123	-.078	.040	.014	-.063
CO2	-.096	-.025	.098	.003	-.029	.021
CO3	.007	.044	-.080	-.040	-.064	-.016
CE1	.146	-.002	-.041	-.010	-.020	.056
CE2	.024	.013	-.058	.016	-.019	.042
CE3	-.076	-.014	.037	-.065	.089	.003
CE4	.061	-.041	-.007	.031	-.007	-.061
ROI1	-.729	.046	.029	.006	-.039	.009
ROI2	.896[a]	-.143	-.090	-.009	.045	-.005
PT1	-.143	.958[a]	-.442	-.078	-.025	-.102
PT2	-.090	-.442	.936[a]	-.413	-.113	.099
PT3	-.009	-.078	-.413	.950[a]	-.256	-.190
PT4	.045	-.025	-.113	-.256	.950[a]	-.464
PT5	-.005	-.102	.099	-.190	-.464	.917[a]
PT6	.050	.008	-.004	-.049	-.074	-.519
PR1	-.018	-.033	.055	.038	-.026	-.007
PR2	6.588E-005	.030	-.001	-.022	.037	-.038
PR3	.066	.046	.024	-.132	.001	-.005
PR4	-.027	-.013	-.024	.044	.010	-.037
PR5	-.051	-.063	-.028	.035	-.018	.060
FC1	-.110	-.038	.093	-.178	.031	.134
FC2	.103	.005	-.078	.018	-.017	-.014
FC3	.090	-.052	-.049	.098	-.087	-.032
BI1	.024	.037	-.134	.154	-.018	-.089
BI2	-.034	-.095	.113	-.099	.056	.042

Anti-image Matrices

	PT6	PR1	PR2	PR3	PR4	PR5
PEoU3	.049	-.032	-.040	.041	-.009	.048
PEoU4	-.068	.067	.001	-.049	.063	-.008
MO1	-.011	-.007	-.005	.051	.019	-.124
MO2	-.127	.019	.005	.001	-.033	.055
CO1	.010	-.015	.020	-.002	.103	-.111
CO2	-.116	.023	-.022	.006	-.014	.054
CO3	.058	-.006	-.011	.038	-.057	-.029
CE1	-.050	.002	.010	-.071	.050	-.075
CE2	-.007	-.010	.004	-.002	.057	-.004
CE3	-.039	-.050	.065	-.058	.031	.014
CE4	.074	.119	-.084	.002	.009	-.001
ROI1	-.023	-.033	.012	.002	.048	-.003
ROI2	.050	-.018	6.588E-005	.066	-.027	-.051
PT1	.008	-.033	.030	.046	-.013	-.063
PT2	-.004	.055	-.001	.024	-.024	-.028
PT3	-.049	.038	-.022	-.132	.044	.035
PT4	-.074	-.026	.037	.001	.010	-.018
PT5	-.519	-.007	-.038	-.005	-.037	.060
PT6	.942[a]	.040	-.045	.164	-.061	-.098
PR1	.040	.717[a]	-.623	-.052	.060	-.011
PR2	-.045	-.623	.723[a]	-.163	-.226	-.214
PR3	.164	-.052	-.163	.805[a]	-.159	-.245
PR4	-.061	.060	-.226	-.159	.825[a]	-.261
PR5	-.098	-.011	-.214	-.245	-.261	.799[a]
FC1	-.103	-.047	.051	-.061	-.022	.271
FC2	.027	.069	.003	-.031	.007	.026
FC3	.033	-.022	.061	-.016	-.060	.021
BI1	.054	.076	-.096	-.018	.062	-.020
BI2	-.070	-.131	.142	-.028	-.068	.079

Anti-image Matrices

	FC1	FC2	FC3	BI1	BI2
PEoU3	.059	-.101	-.046	.070	-.078
PEoU4	-.015	-.034	.081	-.071	.073
MO1	.023	-.010	-.022	-.045	-.049
MO2	.049	-.028	-.093	-.032	.019
CO1	-.109	-.017	.019	.098	-.081
CO2	.022	.053	.048	-.132	.105
CO3	.026	-.053	-.026	.097	-.037
CE1	-.214	-.037	-.025	.093	-.017
CE2	.020	.008	.034	-.146	.118
CE3	.204	-.065	-.127	-.050	.024
CE4	-.178	.090	-.007	.102	-.096
ROI1	.078	-.126	-.025	-.011	-.020
ROI2	-.110	.103	.090	.024	-.034
PT1	-.038	.005	-.052	.037	-.095
PT2	.093	-.078	-.049	-.134	.113
PT3	-.178	.018	.098	.154	-.099
PT4	.031	-.017	-.087	-.018	.056
PT5	.134	-.014	-.032	-.089	.042
PT6	-.103	.027	.033	.054	-.070
PR1	-.047	.069	-.022	.076	-.131
PR2	.051	.003	.061	-.096	.142
PR3	-.061	-.031	-.016	-.018	-.028
PR4	-.022	.007	-.060	.062	-.068
PR5	.271	.026	.021	-.020	.079
FC1	.902[a]	-.279	-.204	-.062	-.110
FC2	-.279	.947[a]	-.185	-.175	.144
FC3	-.204	-.185	.961[a]	-.209	.023
BI1	-.062	-.175	-.209	.892[a]	-.674
BI2	-.110	.144	.023	-.674	.884[a]

a. Measures of Sampling Adequacy(MSA)

Communalities

	Initial	Extraction
PU1	.800	.818
PU2	.825	.872
PU3	.776	.779
PU4	.733	.639
PEoU1	.632	.481
PEoU2	.704	.635
PEoU3	.814	.872
PEoU4	.797	.846
MO1	.655	.562
MO2	.646	.500
CO1	.644	.531
CO2	.760	.520
CO3	.749	.526
CE1	.549	.449
CE2	.747	.781
CE3	.802	.829
CE4	.809	.808
ROI1	.859	.889
ROI2	.821	.907
PT1	.784	.721
PT2	.822	.737
PT3	.836	.821
PT4	.833	.855
PT5	.862	.851
PT6	.785	.754
PR1	.550	.567
PR2	.667	.825
PR3	.363	.308
PR4	.421	.378
PR5	.526	.460
FC1	.594	.433
FC2	.535	.425
FC3	.570	.518
BI1	.759	.844
BI2	.736	.755

Extraction Method: Maximum Likelihood.

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	13.773	39.350	39.350	13.307	38.021	38.021
2	3.500	9.999	49.349	2.984	8.526	46.547
3	2.846	8.132	57.481	2.035	5.815	52.362
4	1.785	5.100	62.581	1.794	5.125	57.486
5	1.672	4.777	67.357	1.690	4.828	62.314
6	1.209	3.455	70.812	.873	2.495	64.808
7	1.081	3.090	73.902	.813	2.323	67.131
8	.911	2.603	76.506			
9	.783	2.236	78.741			
10	.688	1.967	80.708			
11	.640	1.829	82.538			
12	.567	1.620	84.158			
13	.482	1.377	85.535			
14	.475	1.358	86.894			
15	.454	1.297	88.190			
16	.425	1.214	89.404			
17	.386	1.102	90.506			
18	.363	1.037	91.543			
19	.328	.937	92.480			
20	.280	.800	93.280			
21	.260	.744	94.024			
22	.232	.664	94.688			
23	.228	.652	95.340			
24	.199	.567	95.907			
25	.195	.557	96.465			
26	.177	.505	96.969			
27	.166	.475	97.445			
28	.150	.428	97.873			
29	.141	.404	98.277			
30	.125	.358	98.635			
31	.111	.316	98.951			
32	.106	.303	99.254			
33	.098	.281	99.535			
34	.087	.250	99.785			
35	.075	.215	100.000			

Total Variance Explained

Factor	Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %
1	6.383	18.238	18.238
2	3.747	10.706	28.944
3	3.385	9.672	38.616
4	3.277	9.362	47.979
5	2.696	7.703	55.682
6	2.558	7.310	62.992
7	1.449	4.140	67.131
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			

Extraction Method: Maximum Likelihood.

Factor Matrix[a]

	Factor						
	1	2	3	4	5	6	7
PU1	.699						
PU2	.702			.412			
PU3	.675						
PU4	.679						
PEoU1	.446	.490					
PEoU2	.550	.525					
PEoU3	.519	.614					
PEoU4	.512	.593					
MO1	.667						
MO2	.660						
CO1	.685						
CO2	.651						
CO3	.624						
CE1	.544						
CE2	.717						
CE3	.730						
CE4	.751		-.419				
ROI1	.781		-.453				
ROI2	.753		-.417				
PT1	.784						
PT2	.774						
PT3	.759						
PT4	.705	-.433					
PT5	.702	-.420					
PT6	.690						
PR1				.479	.407		
PR2				.508	.554		
PR3							
PR4							
PR5					.434		
FC1	.534						
FC2	.579						
FC3	.618						
BI1	.664					.467	
BI2	.634						

Extraction Method: Maximum Likelihood.

a. 7 factors extracted. 11 iterations required.

Goodness-of-fit Test

Chi-Square	df	Sig.
1354.734	371	.000

Rotated Factor Matrix[a]

	Factor						
	1	2	3	4	5	6	7
PU1				.777			
PU2				.824			
PU3				.755			
PU4				.587			
PEoU1		.603					
PEoU2		.670					
PEoU3		.906					
PEoU4		.890					
MO1		.533					
MO2		.425					
CO1	.505						
CO2	.542						
CO3	.568						
CE1			.518				
CE2			.762				
CE3			.792				
CE4			.711				
ROI1			.491				.674
ROI2							.765
PT1	.710						
PT2	.744						
PT3	.845						
PT4	.896						
PT5	.889						
PT6	.822						
PR1						.740	
PR2						.903	
PR3						.524	
PR4						.575	
PR5						.636	
FC1					.454		
FC2							
FC3					.501		
BI1					.812		
BI2					.758		

Extraction Method: Maximum Likelihood.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 8 iterations.

Factor Transformation Matrix

Factor	1	2	3	4	5	6	7
1	.593	.352	.411	.384	.339	-.026	.305
2	-.560	.701	-.101	.291	.163	-.223	-.151
3	.436	.203	-.517	.216	-.068	.385	-.549
4	-.354	-.307	.032	.611	.049	.593	.226
5	-.041	.493	.191	-.404	-.403	.570	.260
6	-.129	-.044	.264	-.374	.722	.349	-.359
7	-.033	-.062	.668	.209	-.409	-.049	-.579

Extraction Method: Maximum Likelihood.
Rotation Method: Varimax with Kaiser Normalization.