SYNOPSIS OF THE THESIS

Barriers in Adoption of Internet of Things in Manufacturing Industries

Doctoral Thesis Submitted

In partial fulfilment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

In

MANAGEMENT

By

Gurvinder Singh

UID: 16JU11300010

Under the Guidance of

Dr. Tarak Nath Paul
(Research Supervisor)
Assistant Professor
ICFAI University, Jharkhand
Ranchi

Dr. Sushil Kumar Pare
(Research Co-Supervisor)
Assistant Professor
Thakur Institute of Management
Studies & Research, Mumbai

ICFAI UNIVERSITY JHARKHAND

RANCHI

July 2021

CONTENTS

1. INTRODUCTION

The Internet of Things (IoT) has been first defined as a system of interconnected devices (Farooq, 2015). IoT named devices with smart interferences and identities that connect and communicate to add value to their environment and users (Yaqoob et al., 2017). The scope of IoT applications is wide in different areas like smart homes, smart cars, smart buildings, smart manufacturing, environment monitoring, health care systems, energy management, and many more. The IoT and IIoT are similar terms however, the application of IoT in industrial and manufacturing segments is known as the Industrial Internet of Things (IIoT). The IIoT has revolutionized factory and industrial segmentations through its excellence which is the outcome of automation. Far greater efficiency, accuracy, scalability, money-saving, time-saving, predictive maintenance, and many other values are instances of IoT benefits (Zhou, 2017). This emerging phenomenon (IoT) has its concerns for adaptation too. According to Gartner forecast, information security is a top concern among enterprises adopting IoT (Gartner, 2016). Security concerns are the main barrier in adoption due to fear of control on sensitive machinery and controlling systems in industries. Financial loss and confidential data leakage, death, and injuries are the impacts of security threats and cyber-attacks in IoT. Studying IoT security threats in a different application specifically in industrial segmentation is an ongoing research area in academic and industrial surveys. Along with security threats, there are other factors equally important to be considered and have a major impact on the adoption of IoT. As per the UTAUT by Viswanath Venkatesh, four factors playing a significant role in the adoption of technologies, and these factors are Performance Expectancy (PE), Effort Expectancy (EE), Facilitating Conditions (FC), and Social Influence. This research will explore if Security Awareness (SA) impacts the adoption of IoT or

PE, EE and FC also play a role in the decision of IoT adoption in manufacturing companies in and around Mumbai. The study will also explore the impact of the size of the company on these factors.

2. RESEARCH MOTIVATION

The research pieces of literature on IoT indicate that several unresolved issues hinder the adoption of IoT. Several authors indicated that the privacy of sensitive data collected by IoT devices is an issue (Eleanor, 2015). Data collected over RFID raises data integrity issues (Hahn & Govindarasu, 2011). Data travel on wireless mode raises several security concerns which is pointed out by different authors. (Brumfitt et al., 2014). Further, many researchers and authors emphasised on resolving security issues which is hinderance in adoption of IoT (Atzoria, 2010). There are many articles that give attention to resolving security issues which are confining the adoption of IoT.

The researchers have also explored other factors which influence users intention to adopt technology. What is not well known is the influence of security issues and other drivers of consumer acceptance of the IoT technologies (Gao, 2014). The UTAUT model consists of six main constructs, namely Performance Expectancy, Effort Expectancy, Social Effort Expectancy, Social Influence, Facilitating Conditions, behavioural intention to use the system, and usage behaviour. The UTAUT model contains four essential determining components and four moderators. According to the model, the four determining components of BI and usage behaviour are Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Condition

(Venkatesh et al., 2003). Gender, age, experience, and willingness to use are the moderators that affect the usage of technology (Chao, 2019).

As researchers have given different reasons for hindrance in the adoption of IoT in different pieces of literatures while there is a need of consolidated study which explores all reasons together and bring right information to the table. Therefore, the problem this study addresses is identifying the reasons influencing consumers intention to adopt IoT in the manufacturing industry in and around Mumbai. The study analyses, Security Awareness, Performance Expectancy, Effort Expectancy, and Facilitating Conditions. Further, the study will explore if size of the organisation moderates the relationship between dependent and independent variables. The resulting report will help IoT vendors, service providers, and business managers increase IoT adoption.

3. REVIEW OF LITERATURE

List of some of the important literature reviewed for this study along with their link to the study is mention in the table as follows:

Title	**Type**	**Author/ Year**	**Gist**	**Linkage to research**
User acceptance of information technology: A unified view ProQuest Dissertations and Theses;	Research Paper	Venkatesh, Viswanath 1998	This dissertation addresses issues related to user acceptance of technology.	The conclusion of this study that TAM is a best model for user acceptance is adopted in this research.
The impact of security awareness on adopting internet of things ProQuest Dissertations and Theses	Thesis	Allen A. Harper 2016	The research is based on finding the reason if security awareness in U.S. consumers has an impact on users' intention in adoption of IoT. Extended UTAUT model is used.	This research has also use UTAUT model to study the barriers in adoption of IoT in Large, Medium and Small Enterprises in India.
Understanding and Overcoming Barriers to Technology Adoption Among India's Micro, Small and Medium Enterprises	White Paper	Intuit Technology Services Private Limited	In India, medium-sized and large businesses are adopting technology in major ways however small business in India is simply not realising the full potential technology can bring as a game-changer to the old ways of doing things in their businesses.	The target population of research is Large, Medium and Small Enterprises in India hence this white paper provided theoretical reasons of low acceptance of technology adoption in small scale industries.

Title	Type	Author/ Year	Gist	Linkage to research
Research Directions for the Internet of Things IEEE Internet of Things Journal,	White Paper	John A. Stankovic, 2014	Eight key research topics on IoT are enumerated and research problems within these topics are discussed.	This paper helped during initiation of research and identifying the topic.
User Acceptance of Computer Technology	Chapter of book	Davis, Fred, 1989	The research explores people acceptance from the major of their intentions and ability to explain their intention in terms of their attitude, subjective norms, perceived usefulness, perceived ease of use, and related variables.	This research paper provides an understanding of users' intention to adopt computers which is similar to this study to understand users intention to adopt IoT
IoT Safety, Privacy, Security and Ethics	White Paper	A F Atlam, GB Wills 2019	The challenges in IoT safety, Privacy and Ethics.	Security awareness is a main construct so it's important to understand security related challenges.
Cyber Security Challenges in Healthcare IoT Devices.		Arampatzis, A 2019	The cybersecurity impact on healthcare industry where IoT is used intensively	Understanding of security challenges is one of the main constructs of this study

Title	Type	Author/ Year	Gist	Linkage to research
Top 10 Reasons People Aren't Embracing the IoT.	White Paper	Buntz, B. 2016	Identify the reason for slow adoption of IoT	The purpose of this research is to identify reasons for hinderance in IoT adoption.
Malvertising: What You Need to Know to Prevent It.	Web Document	Clean.IO 2020	Understand Malvertising attacks and its related threats	Its related to security awareness construct of this study
Increase in Ransomware Attacks in Q3 2020.	Web Document	Das, S. 2020	What is ransomware attack and how it can impact IoT landscape	Its related to security awareness construct of this study
5 challenges still facing the Internet of Things.	Web Document	D'mello, A. 2020	Security, ethical, governance, monitoring and policy related challenges with IoT environment	The factor explained are related to facilitating conditions that is one of the constructs in the study.
The literature review of technology adoption models and theories for the novelty technology.	White Paper	Lai, P.	The paper describes different model of technology adoptions used by researchers along with its advantages and disadvantages	This paper gave important knowledge to design model of the study

Title	Type	Author/ Year	Gist of Points gained	Linkage to research
Internet of Things security: A survey. Journal of Network and Computer Applications.	White Paper	Fadele Ayotunde Alaba, M. I. 2017	Understand security risks for IoT along with mitigation plans	Its related to security awareness construct of this study
Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges.	White Paper	Fisnik Delipi 2016	How loss of data privacy can impact adoption of IoT	Its helped to understand the data privacy impact on adoption of IoT
The IoT and Next-Generation Monitoring Challenges.	White Paper	Flower, Z. 2016	Monitoring IoT connected devices is another challenge which restrict security solutions.	It is related to security construct and facilitating conditions.
How to Interpret P-values and Coefficients in Regression Analysis. Retrieved	Web Document	Frost J 2019	Understand regression test and correlations	This paper provided knowledge to design data analysis and methodology.
IoT Governance, Privacy and Security Issues, European research cluster on internet of things	Research Paper	Gianmarco Baldini 2015	This research paper was written after a conference on IoT security by IERC. Paper describes the security; data protection and privacy are at core if IoT to be adopted successfully.	IoT related security awareness is one of the constructs hence information of this paper is very useful.

Title	Type	Author/ Year	Gist	Linkage to research
A Simplified Approach to Thesis and Dissertation	Book	Galero-Tejero 2011	Guidelines to write an effective thesis	This book gave insight on writing professional thesis
Ethical Design in the Internet of Things. Springer	White Paper	Gianmarco Baldini 2018	Explained the importance of ethical component while designing IoT solutions	Related to acceptance of IoT
What is a Variance Inflation Factor?	Web Document	Glen, S 2015	Understanding different statistical facts for research data analysis	Related to data analysis of this study
Cronbach's Alpha: Simple Definition, Use and Interpretation.	Web Document	Glen., S 2021	Understand Cronbach's test	Used for data analysis in this study.
Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications	White Paper	I. Yaqoob 2017	Description of different layers of architecture of IoT. The security threats at each layer and security solutions	Different security threats awareness among users which is causing hindrance in the adoption of IoT

Title	Type	Author/ Year	Gist	Linkage to research
Likert scales and data analyses. ResearchGate	White Paper	I.E. Allen and C.A. Seaman. 2017	Description of Likert scale, its advantages and short falls.	Data gathering and analysis for this study
Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research.	Thesis	Icek Ajzen 1975	The study describes users' attitude, intention and behaviour which plays significant role in adoption of anything	It is one of the main components adopted in UTAUT which is base of our study
A unified perspective on the factors influencing consumer acceptance of internet of things technology. Asia Pacific Journal of Marketing and Logistics , 211-231.	White Paper	Lingling Gao 2014	This research paper describes the factors which influences users for the adoption of IoT	Technology adoption model
MSME. What is MSME.	Web Document	2020	Description of MSME organisation by government of India	Segregate organisations into large, medium and small size for analysis
Factor influencing information communication technology acceptance and use in small and medium enterprises in Kenya. Pro Quest.	Thesis	Nyandoro, C. K 2016	The study reveals the factors which influence adoption of ICT in Kenya. The study adopted UTAUT model and concluded facilitating condition plays a significant role.	The research is on same guidelines and adopting some of the constructs used in this thesis.

Title	Type	Author/ Year	Gist of Points gained	Linkage to research
User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly	Thesis	Viswanath Venkatesh 2003	The research explains UTAUT in detail. It explores 8 technology acceptance model developed by previous researchers and explains the advantages and limitations of these models.	The UATUT is the base of the study which is adopted from this research.
Comparison of Quantitative and Qualitative Research Traditions: epistemological, theoretical, and methodological differences. European Journal of Research Development and Policy	White Paper	Yilmaz, K. 2013	Paper explains the research areas where quantitative and qualitative research methods are applicable.	The paper provided knowledge to build research design.
Analysing the Use of UTAUT Model in Explaining an Online Behaviour: Internet Banking Adoption, Department of Marketing and Branding, Brunel University	Thesis	Kholoud Ibrahim Al-Qeisi 2009	The research explains the viability of UATUT model and describes its advantages over rest of the available models.	This research is one of the bases to adopt UATUT

4. RESEARCH GAP

The purpose of this non-experimental correlation study is to measure the correlation, if any, of Security Awareness, Performance Expectancy, Effort Expectancy, and Facilitating Conditions, on the consumer intention to adopt the IoT along with checking if organisation size moderates relationship between these independent variable and dependent variable. An understanding of this relationship is increasingly important as it will reveal the real causes of the slow adoption of IoT which will help IoT vendors and service provides to focus on the right area to improve its adoption. If Security Awareness is the real concern, then the industry needs a more secured solution. However, if other factors like Performance Expectancy, Effort Expectancy, Facilitating Condition are hurdles, then a solution must come to overcome these issues. On the other hand, if the size of the company impacts the Adoption of IoT, the solutions are required to cater to the need of specific size of the manufacturing companies.

The IoT is still an emerging technology and if this study is not performed, a gap would persist in the body of knowledge to know actual reasons which are hindering the adoption of IoT in manufacturing companies. This gap may lead to delay in benefits realization of the IoT. However, by identifying the concrete factors driving adoption of the IoT, changes will be made sooner to increase the adoption rate.

5. RESEARCH OBJECTIVES

The research objective of this study is to develop and validate an extended technology adoption model for the IoT. There are two types of research questions that support the research objective. The primary research question addresses the research topic, the impact of Security Awareness on the Adoption of the IoT. The secondary research questions attempt to identify the other factors in addition to Security Awareness that affects the adoption. The primary and secondary research questions are as follow:

Primary Research Question

- ❖ To what extent, if any, does a consumer's security awareness influence intention to adopt the IoT?
  - ➢ Does size of the organisation moderates relationship between security awareness and intention to adopt IoT?

Secondary Research Questions

The secondary research questions for this topic address the other constructs of the UTAUT (Venkatesh & Thong, 2012) that are Performance Expectancy, Effort Expectancy, and Facilitating Conditions.

- ❖ To what extent, if any, does Performance Expectancy influence consumers' intention to adopt the IoT?

    - Does size of the organisation moderates relationship between performance expectancy and intention to adopt IoT?

- To what extent, if any, does Effort Expectancy influence consumer intention to adopt the IoT?
    - Does size of the organisation moderates relationship between effort expectancy and intention to adopt IoT?

- To what extent, if any, does Facilitating Conditions influence consumers' intention to adopt IoT?
    - Does size of the organisation moderates relationship between facilitating conditions and intention to adopt IoT?

6. RESEARCH HYPOTHESES

Based on objective and research questions, following hypothesis were tested:

$H_{1.0}$: Security Awareness influences consumer intention to adopt the IoT in manufacturing companies in and around Mumbai

$H_{1.1}$: The Organisation Size moderates the relationship between Security Awareness and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai

$H_{2.0}$: Performance Expectancy influences consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

$H_{2.1}$: The Organisation Size moderates the relationship between Performance Expectancy and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

$H_{3.0}$: Effort Expectancy influences consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

$H_{3.1}$: The Organisation Size moderates the relationship between Effort Expectancy and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

$H_{4.0}$: Facilitating Conditions influence consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

$H_{4.1}$: The Organisation Size moderates the relationship between Facilitating Conditions and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.

7. SCOPE OF RESEARCH

Since the IoT is becoming a reality and there remain significant security issues that pose a risk to adoption (Roman et al., 2011). Hence, it’s important to understand the real issues which are impacting the adoption of IoT in the manufacturing industry. The security threat awareness construct will be evaluated along with UTAUT constructs- Performance Expectancy, Effort Expectancy, Facilitating Conditions to bring to the table the real facts which are hampering the adoption of IoT in the manufacturing industry.

The new model having security awareness as a construct with constructs given in the UTAUT model will be leveraged by others and used to better understand the problem/s in the adoption of IoT. This study will help service provides of IoT to understand the reasons for the slow adoption of IoT and give solutions to overcome those issues.

The model which will be developed using UTAUT constructs along with the construct of Security Awareness will be useful for understanding other areas of technology adoption. The same model can be applied to non-manufacturing industries to understand their area of problems in the adoption of IoT and bring the right solutions for them.

This study is limited to manufacturing industries in and around Mumbai however, the same model can be applied to other states and cities to understand the actual obstacles in the adoption of IoT.

Framework of Study

The following framework describes how four independent variables Security Awareness, Performance Expectancy, Effort Expectancy, and Facilitating Conditions will be used to check their relationship with dependent variable adoption of IoT. The size of the organization will be used as a moderator to check its impact on the dependent variable.

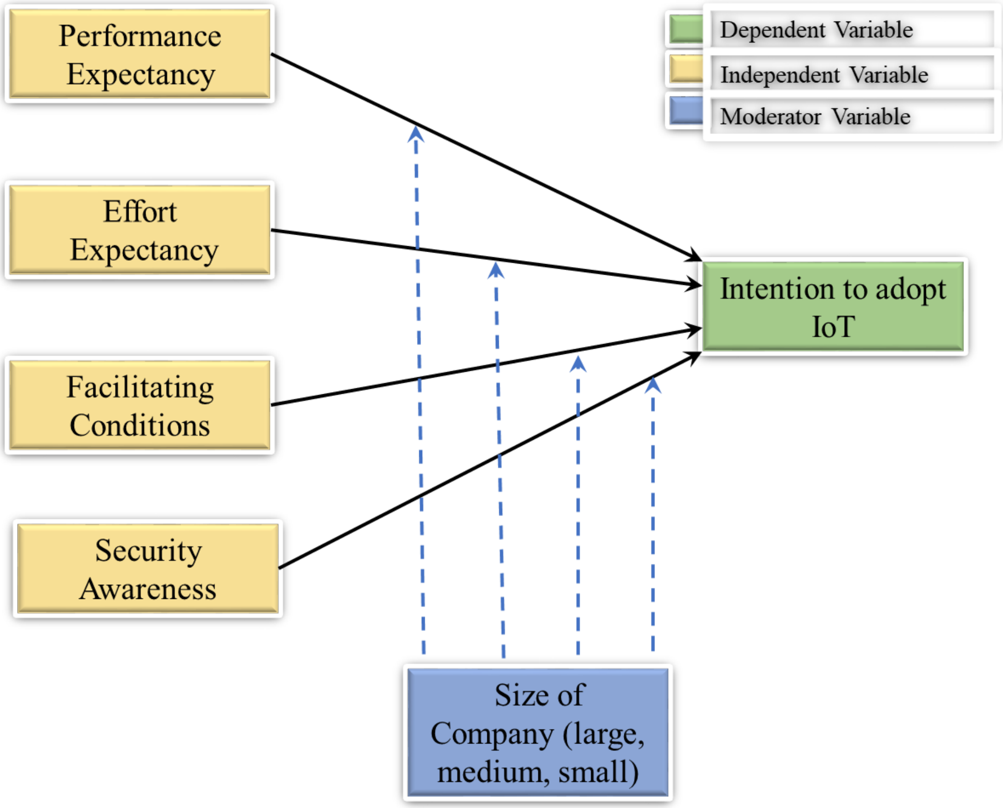

Figure: Framework of Study

Target Group

The target group of the research is owners and senior management who are running large, small, and medium sized manufacturing enterprises in and around Mumbai. The source of contact details is the Ministry of Micro Small and Medium Enterprises office in Delhi.

Criteria for Large, Small and Medium Organisation

As per the Central Government of India notice on 1st June 2020, the criteria for micro, small and medium size industries are as follows (MSME, 2020):

- A micro enterprise, where the investment in plant and machinery or equipment does not exceed one crore rupees and turnover does not exceed five crore rupees.
- A small enterprise, where the investment in Plant and Machinery or Equipment does not exceed ten crore rupees and turnover does not exceed fifty crore rupees.
- A medium enterprise, where the investment in Plant and Machinery or Equipment does not exceed fifty crore rupees and turnover does not exceed two hundred and fifty crore rupees.

The investment in plants and machinery exceeds fifty crores will be treated as a large scale industry.

Sample Size

The sample size was determined using the Slovin's formula (Tejero, 2011).

$n = N / (1 + Ne^2)$

Where:

n = Number of samples,

N = Total population and

e = Error tolerance (level).

The number of manufacturing companies registered in Mumbai as per Ministry of Corporate Affairs are 60,000 approximately. As per Slovin's guidelines, 400 is the appropriate size of samples for such population size.

Seven hundred manufacturing companies are identified to collect samples. The contact details of owners, senior management, and information technology head were collected through different internet sites and social media sites. Out of 700, approximately 600 people were contacted through phone and face to face interview to answer the survey question. The response was received from 500 users approximately. The records with incomplete information were removed and 423 records were validated for analysis as shown in the table.

Sample Size

Industry Type	Small	Medium	Large	Grand Total
Clothing and Textiles	11	10	6	27
Electronics, Computers and Telecommunication	1	1	1	3
Food	58	24	28	110
Leather and Products	1		3	4
Machinery & Equipment	17	55	20	92
Metals & Chemicals	22	90	30	142
Paper & Paper products	4	7	7	18
Petroleum, Oil and Gas	2	2		4
Plastic, Rubber	1			1
Power			2	2
Woods and Products	13	5	2	20
Grand Total	**130**	**194**	**99**	**423**

Data Collection

The primary data is collected through statements designed in schedule that were asked to the respondents through face to face interview or phone. Five-point Likert scales is used for collection of data in pilot as well as the main study. Research confirms that data from Likert items (and those with similar rating scales) becomes significantly less accurate when the number of scale points drops below five or above seven (Johns, 2010). The responses were collected based on five options: ‘Strongly agree, Agree, Neutral, Disagree and Strongly disagree’. The secondary data that is organisation financial status and number of employees are collected through the Ministry of MSME, third party and through websites. The secondary data is also verified during interviews where participants were ready to share information.

8. RESEARCH METHODOLOGY

The research method chosen for this study is a quantitative, non-experimental, correlational study using regression as the form of data analysis. There are two types of studies recommended by researchers – quantitative and qualitative. The quantitative method for this study is most suitable as data received from the survey will be converted into numbers for analysis. Quantitative research, in contrast to qualitative research, deals with data that are numerical or that can be converted into numbers (Sheard, 2010). Due to the nature of the research questions, a quantitative study is used to show the relationship between different constructs.

Data is be collected through a survey. A survey is a common form of instrument used in non-experimental studies, whereby the constructs are explored through close-ended questions. A correlational study was selected to determine the relationship between dependent and independent variables.

Subsequently, A quantitative non-experimental correlational study will be designed, and multiple regression will be used for data analyses as follows:

- Reliability test of the independent variables using Cronbach's alpha.
- Multicollinearity test for each independent variable through Variance Inflation Factor (VIF).
- Remove outliers from data with Interquartile Range (IQR).
- Correlation of independent and dependent variables.
- Multiple regression test of all independent variables with the dependent variable.
- Build interaction variable from each size of the organisation and independent variable.
- Multiple regression test for interaction variables and dependent variable.

9. RESEARCH DATA ANALYSIS

The test results and its analysis are explained as follows:

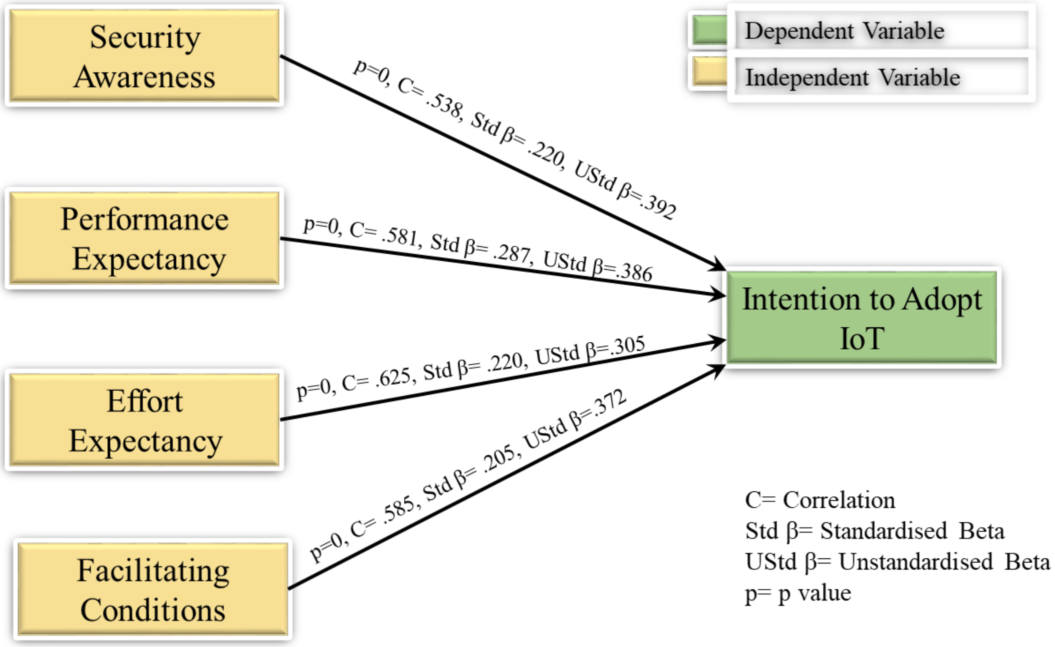

Figure 9-1: Research Model Independent and Dependent Variable

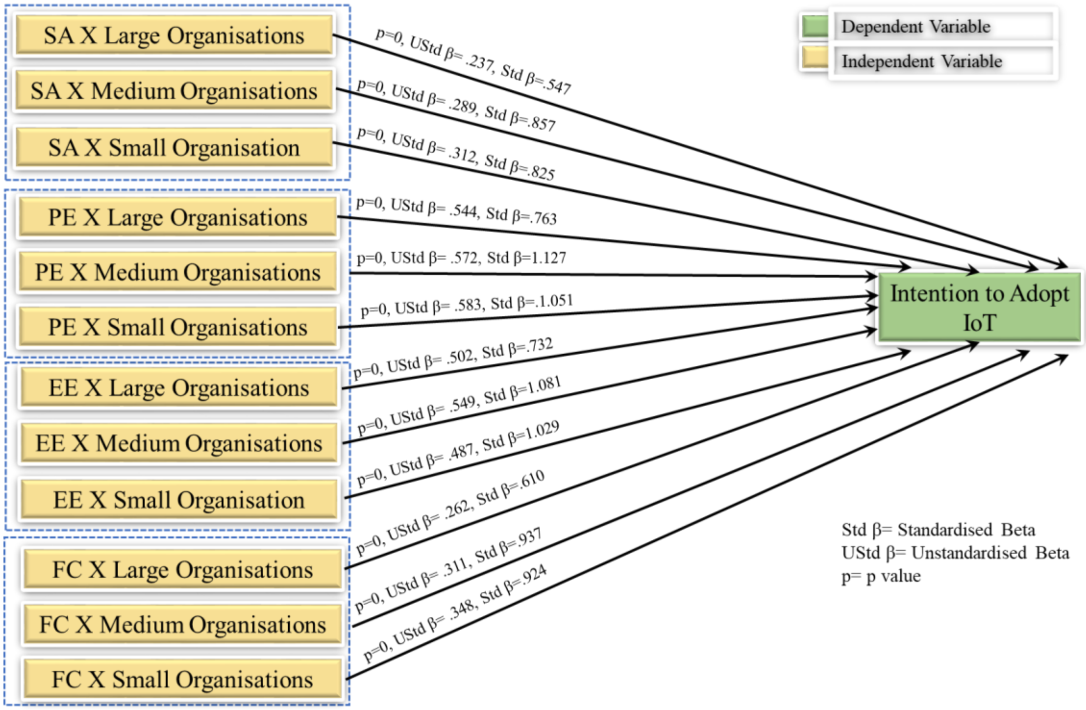
SA X Large Organisations
SA X Medium Organisations
SA X Small Organisation
PE X Large Organisations
PE X Medium Organisations
PE X Small Organisations
EE X Large Organisations
EE X Medium Organisations
EE X Small Organisation
FC X Large Organisations
FC X Medium Organisations
FC X Small Organisations
Intention to Adopt IoT
p=0, UStd β= .237, Std β=.547
p=0, UStd β= .289, Std β=.857
p=0, UStd β= .312, Std β=.825
p=0, UStd β= .544, Std β=.763
p=0, UStd β= .572, Std β=1.127
p=0, UStd β= .583, Std β=.1.051
p=0, UStd β= .502, Std β=.732
p=0, UStd β= .549, Std β=1.081
p=0, UStd β= .487, Std β=1.029
p=0, UStd β= .262, Std β=.610
p=0, UStd β= .311, Std β=.937
p=0, UStd β= .348, Std β=.924
🟩 Dependent Variable
🟨 Independent Variable
Std β= Standardised Beta
UStd β= Unstandardised Beta
p= p value

Figure 9-2: Research Model with Interaction variable

$H_{1.0}$: The test results show p value of 0 which concludes Security Awareness is statistically significant. The correlation value of .538 shows positive correlation and proves security awareness influence on the adoption of IoT. Further regression test shows standardised beta value of .220 and unstandardised bite value of .392 and prove the influence but it’s not very high.

$H_{1.1}$: Further analysis table proves that small, medium and large size organisations moderate the relationship as p value for all variables is 0. The influence of small and medium size organisations is higher as compare to large size organisation as standardised coefficient values for interaction variable with small and medium size organisation is higher than interaction variable build with large size organisation.

$H_{2.0}$: Like above hypothesis the relationship between performance expectance and intention to use IoT is tested through correlation and value of .581 proves positive correlation. The regression test shows standardised beta value of .287 and unstandardized beta value of .387 which shows influence of performance expectancy.

$H_{2.1}$: To check if organisation size moderates relationship, the correlation results explain significance of each interaction variables on intention to use IoT as p value is 0 for each variable. The standardised values for each interaction variable are also high that infer the strong relationship between variables.

$H_{3.0}$: The correlation result proves relationship between Effort expectancy and intention to use IoT and value is .625. The p value is 0 in above in regression test that explains statistically significance of the model and standardised coefficient value of .305 and unstandardised value of .220 infer the moderate level of influence of efforts expectancy on Intention to use IoT.

$H_{3.1}$: Further, regression test with interaction variables to check influence of size of the organisation, proves all size of organisations moderates the relationship between Effort Expectancy and Intention to use IoT.

$H_{4.0}$: The correlation value of .585 between facilitating conditions and intention to adopt IoT proves positive correlations. In regression test, the standardised value of .372 and unstandardised value of .205 influence of facilitating condition of intention to adopt IoT.

$H_{4.1}$: In regression test to find if organisation size influence relationship between facilitating conditions and intention to adopt IoT, the standardised value of .610 and unstandardised value of .262 proves this influence.

10. FINDINGS AND CONCLUSIONS

The findings from the result of the study and literature analysis give the following conclusion

Security Awareness

The literature studies gave two views on the consumer security awareness. The first view explains that users are aware of the security threats which is depleting the adoption of technologies. The second view decipher that users take security as granted. Some of the literature stated that users often trade privacy and security for convenience. The results of the study explain the difference in opinions found from the second view and support first view. The correlation and regression test between security awareness and adoption of IoT confirms it. Further, analysis revealed that large, medium, and small size organisations are concerned with security related threats. The medium and small size organisations are more concerned as compare to large size organisations. The reason could be large size organisations have budget and expertise to build security provisions that reduces the fear of security threats. Even though cyber security spending is growing year-on-year with almost 9 per cent growth in 2019, IT security budgets for small and medium businesses and enterprises have gone down and are below the average spend.

Performance Expectancy

For performance expectancy, there are two schools of thoughts, most of the literature explains that performance expectancy improves with adoption of new technologies. Such literatures demonstrate that performance expectancy is most influential construct in user intention to adopt IoT. However, there are literatures that contradict this through. The reason for not selecting performance expectancy by industry could be due to the availability of automation and high-end machines that could deliver high performance without IoT involvement. The other school of thought says that by improving the manufacturing processes, the improved performance can be achieved. Lean Manufacturing adopted by Toyota has improved performance significantly. Lean manufacturing methodology offers increasing quality, reducing costs, shortening lead-times are many benefits which improve the overall efficiency of companies.

The results of this study support first School of thought. The correlation results prove relationship between performance expectancy and intention to adopt IoT. The next phase of study to check which size of organisation moderate relationship between two variables explains all sizes of the organisations influence relationship between performance expectancy and intention to adopt IoT. hence, study concludes performance expectancy plays significant role in consumer intention to adopt IoT.

Effort Expectancy

Similarly, the literature on effort expectancy supports influence on adoption of IoT as well as give contradicting statements. The IoT landscape is highly interactive, ubiquitous, and selfsufficient using smart technology which results in no human interaction. The consumers do not need to put in efforts to use IoT. Therefore, the requirement of learning and attaining knowledge is not there. Smart car is one of the examples to support it. The consumers do not need to get skills to drive a smart car and they still can enjoy the services. As IoT is providing benefits without demanding efforts from consumers that can reduce the significance of effort expectancy. Contrarily, other thought concludes high significance of this construct. The finding form literatures are demonstrating that effort expectancy (i.e. consumers perceive it an "ease of use") is most important determinant that has a direct and strong influence on consumers‟ behavioural intention to adopt technologies.

The results of this study concludes that effort expectancy has relationship with intention to adopt IoT. Hence, study supports second view of literature that effort expectancy plays significant role to influence consumer intention to adopt IoT. Further analysis explained that large, medium as well as small size organisations moderates relationship between effort expectancy and intention to use IoT which concludes construct significance in all size of the organisations.

Facilitating Conditions

As per literatures facilitating conditions are very important aspect to influence consumer intention to adopt IoT. Almost all research papers and studies revealed that it's one of the most important constructs in adoption of technologies.

Data analysis of this study also provide same findings. There is a relationship between facilitating condition and consumer intention to adopt IoT. Further analysis revealed all size of the organisations influence the relationship between facilitating conditions and consumer intention to adopt IoT. The medium and small size organisations have very strong influence while large size organisation influence moderately. As large size organisations have resources due to higher budget that could be a reason for lower influence in comparison to medium and small size organisations.

11. RESEARCH CONTRIBUTION

This study has been performed to explore the reasons which impact the adoption of IoT in manufacturing organizations. Some authors explained security awareness is the main concern for the adoption of IoT. Some of the authors have explored other factors too. This study is a combination of three factors which are taken from the Unified Theory of Acceptance and Use of Technology (UTAUT) by Viswanath Venkatesh along with Security Awareness and Organization Size. The five factors studied are Performance Expectancy, Effort Expectancy, Facilitating Conditions, Security Awareness and Organization Size which is unique in the nature and would be useful for IoT service providers and manufacturing industry to improve productivity and reduce cost of the production particularly in small scale sector.

Contribution for IoT Service Providers

With this study, the IoT service providers can understand the area where they need to focus on to improve the adoption of IoT. and enhance profitability by increasing sale.

Contribution for Manufacturing Organisations

While service providers will show IoT benefits to the organisations, the adoption od IoT will enhance productivity and reduce cost of the operations and manufacturing.

Contribution for Researchers

The researchers can take advance from this research for future studies as follows:

The study is performed on manufacturing companies in Mumbai and nearby areas. The same study can be extended to other geography using location as an independent variable to check the impact on changing the location. The same study will be applicable for other industries too to take benefit from.

As this study explained that security awareness is not impacting the adoption of IoT which is contradicting to different authors who concluded that security awareness has an impact on the adoption of IoT. Hence, the security awareness independent variable can be further explored by adding more parameters like security fatigue to better understand the paradox between security awareness and IoT adoption.

12.LIMITATIONS OF THE RESEARCH

Following are the limitations identified of this research:

- ❖ It is understood that the researcher does not have wide experience performing quantitative studies. Though, research guidelines are followed, design and statistical analysis principles are adhered to perform a valid study. Further, assistance from research guides, university research committee, other researchers, and experts of the field is taken to validate the study.
- ❖ This study is conducted on manufacturing companies in and around Mumbai. Mumbai is a developed city where IoT and security service vendors are available. A similar study conducted in the non-metro cities might give different results.

- The factors considered for this study are very important that are adopted by many researchers for the adoption of technologies. However, some of the researchers have explored additional factors like security fatigue which is not evaluated in this study. The NIST (National Institute for Standards and Technology) defines security fatigue as a weariness or reluctance to deal with computer security (Kassner, 2020).
- The impact of competitors on the adoption of IoT is also not explored in this study.

13.SCOPE FOR FUTURE WORK

- First, the study should be repeated after some time as IoT awareness is increasing and users will be more aware of security risks associated with IoT. Specifically, media, newspapers, and magazines may increase focus on security issues and change the viewpoint of users over time.
- The study is performed on manufacturing companies in Mumbai and nearby areas. The same study can be extended to other geography using location as an independent variable to check the impact on changing the location. The same study will be applicable for other industries too to take benefit from.
- As this study explained that security awareness is not impacting the adoption of IoT which is contradicting to different authors who concluded that security awareness has an impact on the adoption of IoT. Hence, the security awareness independent variable can be further explored by adding more parameters like security fatigue to better understand the paradox between security awareness and IoT adoption.

BIBLIOGRAPHY

1. A F Atlam, G. B. (2019). IoT Safety, Privacy, Security and Ethics. *Research Gate*, 154-157.
2. Ahmed Alenezi, N. H. (2017). The Impact of Cloud Forensic Readiness on Security. *Research Gate*.
3. Ajzen, I. (1991). Organizational Behavior and Human Decision. In I. Ajzen, *The Theory of Planned Behavior," Organizational Behavior and Human Decision Processes* (pp. 178-211).
4. Alexey Medvedev, F. A. (2015). Waste Management as an IoT-Enabled Service in Smart Cities. *Conference on Internet of Things and Smart Spaces* (pp. 104-115). St. Petersburg, Russia: Springer.
5. All, I. F. (2019, March 29). *https://www.iotforall.com*. Retrieved from 7 Challenges of IoT Software Development: https://www.iotforall.com/iot-software-development-challenges
6. Almaiah, M. A. (2019, December 16). *Applying the UTAUT Model to Explain the Students' Acceptance of Mobile Learning in Higher Education.* Retrieved from https://ieeexplore.ieee.org: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8918396
7. Al-Qeisi, K. I. (2009, March). *Analyzing the Use of UTAUT Model in Explaining an Online.* Retrieved from https://core.ac.uk: https://core.ac.uk/download/pdf/40049467.pdf
8. Anand, S. (2020, January 2). *Cyber Security*. Retrieved from https://www.business-standard.com: https://www.business-standard.com/article/companies/despite-growth-in-spending-cybersecurity-budget-dips-for-small-medium-biz-120010100845_1.html

9. Aniket Marathe, M. A. (2018). Internet of Things: Opportunities and applications in pharmaceutical manufacturing and logistics. *Research Gate*.

10. Arampatzis, A. (2019, June 19). *Cyber Security Challenges in Healthcare IoT Devices*. Retrieved from https://www.tripwire.com: https://www.tripwire.com/state-of-security/security-data-protection/iot/cyber-security-healthcare-iot

11. Atoui, R. (2020, November 3). *IoT Security in the Medical Industry*. Retrieved from https://www.iotforall.com: https://www.iotforall.com/iot-security-medical

12. Bednarz, A. (2018, January 30). *What is microsegmentation? How getting granular improves network security*. Retrieved from NetworkWorld: https://www.networkworld.com/article/3247672/what-is-microsegmentation-how-getting-granular-improves-network-security.html

13. Bhandari, A. (2020, March 20). *Analytics Vidya*. Retrieved from https://www.analyticsvidhya.com: https://www.analyticsvidhya.com/blog/2020/03/what-is-multicollinearity/

14. Bilal, M. (2019). *https://arxiv.org/ftp/arxiv/papers/1708/1708.04560.pdf*. Retrieved from https://arxiv.org: https://arxiv.org/ftp/arxiv/papers/1708/1708.04560.pdf

15. Buntz, B. (2016, April 20). *Top 10 Reasons People Aren't Embracing the IoT*. Retrieved from https://www.iotworldtoday.com: https://www.iotworldtoday.com/2016/04/20/top-10-reasons-people-aren-t-embracing-iot/

16. Chao, C.-M. (2019, July 16). *Factors Determining the Behavioral Intention to Use Mobile Learning: An Application and Extension of the UTAUT Model.* Retrieved from https://www.frontiersin.org: https://doi.org/10.3389/fpsyg.2019.01652

17. Chao, C.-M. (2019). *https://www.frontiersin.org/articles/*. Retrieved from https://www.frontiersin.org/articles/: https://www.frontiersin.org/articles/10.3389/fpsyg.2019.01652

18. Chaudhury, A. (2018). *Predictive Maintenance for Industrial IoT of Vehicle Fleets using Hierarchical Modified Fuzzy Support Vector Machine*. Retrieved from https://arxiv.org: https://arxiv.org/ftp/arxiv/papers/1806/1806.09612.pdf

19. Chowdhury, A. (2016). Priority based and secured traffic management system for emergency vehicle using IoT. *2016 International Conference on Engineering and MIS.* Agadir, Morocco: IEEE.

20. Clean.IO. (2020). *Malvertising: What You Need to Know to Prevent It*. Retrieved from https://www.clean.io: https://www.clean.io/malvertising

21. Cronbach, L. J. (2004). *My Current Thoughts on Coefficient Alpha and Successor Procedures.* Los Angeles: University of California. Retrieved from https://files.eric.ed.gov/fulltext/ED483410.pdf

22. Das, S. (2020, November 16). *40% Increase in Ransomware Attacks in Q3 2020*. Retrieved from https://securityboulevard.com: https://securityboulevard.com/2020/11/40-increase-in-ransomware-attacks-in-q3-2020/

23. Davis, D. (1993). User Acceptance of information technology. *Int. J Man- Machine Studies*, 475-487.

24. Davis, M. (2020, April 14). *IoT Tech Expo*. Retrieved from https://www.iottechexpo.com: https://www.iottechexpo.com/2020/04/connected-industry/blog-barriers-to-iot-adoption/

25. Debajyoti Pal, S. F., & Kanthamanon, P. (2018, February 22). *Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective.* Retrieved from https://ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/8300511

26. Deloitte. (2021). *Small Scale Business Trend.* Retrieved from https://www2.deloitte.com: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html

27. D'mello, A. (2020, June 3). *5 challenges still facing the Internet of Things*. Retrieved from https://www.iot-now.com: https://www.iot-now.com/2020/06/03/103228-5-challenges-still-facing-the-internet-of-things/

28. DSM. (2020, July 8). *5 best ways to prevent DDoS attacks*. Retrieved from https://www.dsm.net: https://www.dsm.net/it-solutions-blog/prevent-ddos-attacks

29. Eisley Dizon, B. P. (2021, February 24). *Smart streetlights in Smart City: a case study of Sheffield.* Retrieved from https://link.springer.com: https://link.springer.com/article/10.1007/s12652-021-02970-y

30. Eleanor. (2015, July). *Majority of Consumers Want to Own the Personal Data Collected from their Smart Devices [SURVEY]*. Retrieved from https://trustarc.com: https://trustarc.com/blog/2015/01/05/majority-consumers-want-own-personal-data-survey/

31. Eric Hittinger, P. J. (2019). Internet of Things: Energy boon or bane. *ScienceMag, Vol. 364, Issue 6438*, 326-328.

32. Fadele Ayotunde Alaba, M. I. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 10-28. Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455

33. Fahad Khan, M. A. (2020, February). *oT Based Power Monitoring System for Smart Grid Applications.* Retrieved from Researchgate.com: 10.1109/ICEET48479.2020.9048229

34. Fireeye. (2020). *Anatomy of Advanced Persistent Threats*. Retrieved from https://www.fireeye.com: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

35. Fisnik Delipi, S. Y. (2016). Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. *ResearchGate*.

36. Flower, Z. (2016, December 13). *The IoT and Next-Generation Monitoring Challenges*. Retrieved from https://www.pagerduty.com: https://www.pagerduty.com/blog/iot-monitoring-challenges/

37. Formplus. (2004, December). *Formplus*. Retrieved from https://www.formpl.us: https://www.formpl.us/blog/correlational-research

38. Frost, J. (2021). *How to Interpret P-values and Coefficients in Regression Analysis*. Retrieved from https://statisticsbyjim.com: https://statisticsbyjim.com/regression/interpret-coefficients-p-values-regression/

39. Fruhlinger, J. (2020, January 17). *What is information security? Definition, principles, and jobs*. Retrieved from https://www.csoonline.com: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

40. Galero-Tejero. (2011). A Simplified Approach to Thesis and Dissertation . In Galero-Tejero, *A Simplified Approach to Thesis and Dissertation* (pp. 43-44). Mandaluyong City: National Book Store.

41. Ganti, A. (2021, March 31). *Central Limit Theorem (CLT).* Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/c/central_limit_theorem.asp#:~:text=Key%20Takea

ways-,The%20central%20limit%20theorem%20(CLT)%20states%20that%20the%20distribution%20of,the%20sample%20size%20gets%20larger.&text=A%20key%20aspect%20of%20CLT,population%20me

42. Gartner. (2016). *Forecast: IoT Security, Worldwide, 2016*. Retrieved from https://www.gartner.com/en/documents/3277832/forecast-iot-security-worldwide-

43. Gavin Hull, H. J. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Springer*.

44. Geoffrey Wylde, C. D. (2020). Accelerating the Impact of Industrial IoT in small and medium size business. *World Econimic Forum.* Geveva, Switzerland: World Economic Forum.

45. Gianmarco Baldini, M. B. (2018). Ethical Design in the Internet of Things. *Springer*, 905-925.

46. Glen, S. (2015, September 21). *What is a Variance Inflation Factor?* Retrieved from https://www.statisticshowto.com: https://www.statisticshowto.com/variance-inflation-factor/

47. Glen., S. (2021). *Cronbach's Alpha: Simple Definition, Use and Interpretation*. Retrieved from https://www.statisticshowto.com: https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/

48. Gonçalo Marques, R. P. (2019). Noise Monitoring for Enhanced Living Environments Based on Internet of Things. *World Conference on Information System and Technology* (pp. 45-54). Springer.

49. Griffin, L. (2020). *What is Data Tampering? - Definition & Prevention*. Retrieved from https://study.com: https://study.com/academy/lesson/what-is-data-tampering-definition-prevention.html

50. Grizhnevich, A. (2018, May 3). *IoT for Smart Cities: Use Cases and Implementation Strategies*. Retrieved from https://www.scnsoft.com: https://www.scnsoft.com/blog/iot-for-smart-city-use-cases-approaches-outcomes

51. Hahn, A., & Govindarasu, M. (2011). Cyber Attack Exposure Evaluation Framework for the Smart Grid. *IEEE*, 835-843.

52. Hall, C. (2018, May 8). *IT Pro Today*. Retrieved from https://www.itprotoday.com: https://www.itprotoday.com/iot/survey-shows-linux-top-operating-system-internet-things-devices

53. Hanan Aldowah, S. U. (2019, July). *Security in Internet of Things: Issues, Challenges, and Solutions*. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/326579980_Security_in_Internet_of_Things_Issues_Challenges_and_Solutions

54. Harper, A. (2020). *10 bigget security challanges for IoT*. Retrieved from https://www.peerbits.com: https://www.peerbits.com/blog/biggest-iot-security-challenges.html

55. Harper, A. A. (2016, October). *The Impact of Consumer Security Awareness of Adoption of Internet of Things.* Retrieved from https://pqdtopen.proquest.com/pubnum: https://pqdtopen.proquest.com/pubnum/10196140.html

56. Harper, A. A. (2016). The impact of consumer security awareness on adopting IoT. *Proquest*, 16.

57. Hedges, L. V. (2013). Recommendations for Practice: Justifying Claims of Generalizability. *ResearchGate*.

58. Helen Angela Brumfitt, D. R. (2014). *A Framework for Device Security in the Internet of Things.* Retrieved from http://www.cms.livjm.ac.uk: http://www.cms.livjm.ac.uk/PGNet2014/papers/1569961261.pdf

59. Howard, D. M. (n.d.). *Introduction to Cronbach's Alpha*. Retrieved from https://mattchoward.com: https://mattchoward.com/introduction-to-cronbachs-alpha/

60. I.E. Allen and C.A. Seaman. (2007). Likert scales and data analyses. *ResearchGate*, 64-65.

61. Icek Ajzen, M. F. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. In M. F. Icek Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.*

62. IDC. (2019, October 28). *IDC*. Retrieved from https://www.idc.com: https://www.idc.com/getdoc.jsp?containerId=prUS45612419

63. IOWA, C. I. (n.d.). *What is confidential data?* Retrieved from https://iso.iowa.gov: https://iso.iowa.gov/faq/what-confidential-data

64. Irena Bojanova, G. H. (2014, June 6). *Imagineering an Internet of Anything*. Retrieved from https://ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/6838944

65. Irwin, L. (2020, April 16). *The 5 most common types of phishing attack*. Retrieved from IT Governance: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

66. i-Scoop. (2015, April). *IIoT- the Industrial Internet of Things (IIoT) explained*. Retrieved from https://www.i-scoop.eu: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/industrial-internet-things-iiot/

67. J. Zhou, Z. C. (2017). *Security and Privacy for Cloud-Based IoT.* IEEE Communications Magazine.

68. Jennie Pena, M. L. (2017, April 27). *The Conditional Indirect Effect of Performace Expectancy in use of Facebook, Instagram and Twitter.* Retrieved from http://www.revistalatinacs.org: http://www.revistalatinacs.org/072paper/1181/31en.html

69. Jibran Saleem, M. H. (2018). IoT standardisation: challenges, perspectives and solution. *Association of computing Machinery*, 1-9. Retrieved from https://dl.acm.org: https://dl.acm.org/doi/10.1145/3231053.3231103

70. Johns, R. (2010, March). *Likert Items and Scales.* Retrieved from https://ukdataservice.ac.uk: https://ukdataservice.ac.uk/media/262829/discover_likertfactsheet.pdf

71. José L. Hernández-Ramos, J. B. (2015, July 1). *Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things*. Retrieved from https://www.mdpi.com/1424-8220/15/7/15611: https://doi.org/10.3390/s150715611

72. Juan Jim Tan, S. P. (2007). A Semantic Approach to Harmonizing Security Models for Open Services. *Applied Artificial Intelligence*, 353-379. Retrieved from https://doi.org/10.1080/08839510500484298

73. Jungwoo Lee, S. I. (2011, October). *Adoption of Internet Technology for small business.* Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/266607952_Adoption_of_Internet_Technologies_in_Small_Business

74. Kassner, M. (2020, December 22). *How to address security fatigue and stop cybercriminals from winning*. Retrieved from https://www.techrepublic.com: https://www.techrepublic.com/article/how-to-address-security-fatigue-and-stop-cybercriminals-from-winning/

75. Labram, J. (2016, November 2). *AZO Sensors*. Retrieved from https://www.azosensors.com: https://www.azosensors.com/article.aspx?ArticleID=705

76. Lai, P. (2017). The Litrature Review of Technology Adoption Models and Theories for the Novelty Technology. *Journal of Information Systems and Technology Management*, 21-38.

77. Levinson, M. (2012, February 10). *CIO*. Retrieved from https://www.cio.com: https://www.cio.com/article/2448967/6-ways-to-defend-against-drive-by-downloads.html

78. Levitt, T. (2015). IoT Governance, Privacy and Security Issues. *European Research Cluster on the Internet of Things*.

79. Lingling Gao, X. B. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics* , 211-231.

80. Luigi Atzori, A. I. (2010, May). *The Internet of Things: A Survey*. Retrieved from https://www.cs.mun.ca: https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf

81. Luigi Atzoria, A. L. (2010, October 28). *The Internet of Things: A survey.* Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S1389128610001568?via%3Dihub

82. M. Farooq, M. W. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 1-6.

83. Mary R.Lind, R. W. (1989). Microcomputer adoption — The impact of organizational size and structure. *Science Direct- Volume 16, Issue 3*, 157-162. Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/0378720681900690

84. McNeese, D. B. (2016, February). *SPC Excel*. Retrieved from https://www.spcforexcel.com: https://www.spcforexcel.com/knowledge/basic-statistics/are-skewness-and-kurtosis-useful-statistics

85. Michael Friedewalda, O. R. (2011). Ubiquitous computing: An overview of technology impacts. *Science Direct*, 55-65.

86. Micro, T. (2020). *Exploit Kit*. Retrieved from https://www.trendmicro.com: https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit

87. Micro, T. (2020, May 28). *Smart Yet Flawed: IoT Device Vulnerabilities Explained*. Retrieved from https://www.trendmicro.com: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained

88. Mohamed Abdel Basset, G. M. (2018). Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Generation Computer System* (pp. 614-628). Elsevier. Retrieved from El.

89. Morley, H. R. (2018, January 11). *Shippers embrace Maersk reefer tracker*. Retrieved from https://www.joc.com: https://www.joc.com/international-logistics/cool-cargoes/shipper-embrace-maersk-reefer-tracker-shows-visibility-demand-0

90. MSME, M. o. (2020, July 1). *What is MSME*. Retrieved from https://msme.gov.in: https://msme.gov.in/sites/default/files/MSME_gazette_of_india.pdf

91. Mukherjee, S. (2018, December). *Challenges to Indian micro small scale and medium enterprises in the era of globalization*. Retrieved from research gate: 10.1186/s40497-018-0115-5

92. Mykola, O. (2020, April 29). *Healthcare IoT Security: Risks, Rules, Best Practices, and Our Advice*. Retrieved from https://www.aimprosoft.com: https://www.aimprosoft.com/blog/iot-security-in-healthcare-software-development/

93. Norton. (2018, January 18). *7 tips to prevent ransomware*. Retrieved from https://us.norton.com: https://us.norton.com/internetsecurity-malware-7-tips-to-prevent-ransomware.html

94. Nory Jones, C. M. (2020, January). *Can the IoT helps small business?* Retrieved from Research gate: 10.1177/0270467620902365

95. Nyandoro, C. K. (2016). Factor influencing information communication technology acceptance and use in small and medium enterprises in Kenya. *Pro Quest*, January.

96. Paul C Nystroma, K. R. (2002, September). *Organizational context, climate and innovativeness: adoption of imaging technology.* Retrieved from Sciencedirect.com: https://doi.org/10.1016/S0923-4748(02)00019-X

97. Petchko, K. (2018). Chapter 13 - Data and Methodology. In K. Petchko, *How to Write About Economics and Public Policy* (pp. 241-270). Acadmic Press.

98. Peter, J. (2020, March 29). *What is DDoS Attack*. Retrieved from https://www.varonis.com: https://www.varonis.com/blog/what-is-a-ddos-attack

99. Pulagam, S. (2020, June 6). *How to detect and deal with Multicollinearity*. Retrieved from https://towardsdatascience.com: https://towardsdatascience.com/how-to-detect-and-deal-with-multicollinearity-9e02b18695f1

100. Quebec. (2020). *Definition of the concept of safety*. Retrieved from https://www.inspq.qc.ca: https://www.inspq.qc.ca/en/quebec-collaborating-centre-safety-promotion-and-injury-prevention/definition-concept-safety

101. Rahul Dagar, S. S. (2018, July 12). *Smart Farminig In IoT infrastructure.* Retrieved from IEEE: 10.1109/ICIRCA.2018.8597264

102. Rana Asif Rehman, B. K. (2018). *https://www.researchgate.net/publication/327272757*. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/327272757

103. Rana, M. M., Xiang, W., Wang, E., & Jia, M. (2017, December 8). *IoT Infrastructure and Potential Application to Smart Grid Communications*. Retrieved from https://ieeexplore.ieee.org/: https://ieeexplore.ieee.org/document/8254511

104. Reed, D. (2020, September 14). *Advance Network Services*. Retrieved from https://resources.anscorporate.com: https://resources.anscorporate.com/monitoring-and-maintenance-of-iot-devices

105. RFIC. (n.d.). *RFIC*. Retrieved from https://rficsolutions.com: https://rficsolutions.com/iot/#:~:text=What%20is%20IOT%3F,things%2C%20and%20between%20things%20themselves.

106. Rodrigo Roman, P. N. (2011, September). *Securing the Internet of Things*. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/220475753_Securing_the_Internet_of_Things

107. Rogers, E. M. (2019). *Diffusion of Innovations.* Mahway, MJ: Lawrence Erlbaum Associates.

108. Roman, R., Najera, P., & Lopez, J. (2011, September). *Securing the Internet of Things*. Retrieved from https://ieeexplore.ieee.org/document/6017172: https://ieeexplore.ieee.org/document/6017172

109. Rosencrance, L. (2019, June). *TechTarget*. Retrieved from Top 10 types of information security threats for IT teams: https://searchsecurity.techtarget.com/feature/Top-10-types-of-information-security-threats-for-IT-teams

110. Rouse, M. (2019, May). *https://searchsecurity.techtarget.com/definition/zero-day-vulnerability*. Retrieved from https://searchsecurity.techtarget.com: https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

111. Rouse, M. (2020, July). *industrial internet of things (IIoT)*. Retrieved from https://internetofthingsagenda.techtarget.com: https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

112. Sachin Babar, A. S. (2011). Proposed Embedded Security Framework for Internet of Things (IoT). *ResearchGate*.

113. Saputo, P. (n.d.). *Electronic Data Tampering*. Retrieved from https://saputo.law: https://saputo.law/criminal-law/texas/electronic-data-tampering/

114. Sarah Wray, C. E. (2016, September). *https://inform.tmforum.org*. Retrieved from https://inform.tmforum.org/news/2016/09/60-iot-devices-falling-short-privacy-data-protection/: https://inform.tmforum.org/news/2016/09/60-iot-devices-falling-short-privacy-data-protection/

115. Sarin, A. (2018, April 11). *Legal Issues Pertaining To Internet of Things (IOT)*. Retrieved from https://www.iiprd.com: https://www.iiprd.com/legal-issues-pertaining-to-internet-of-things-iot/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

116. SCHNEIER, B. (2014, January). *Security Risks of Embedded Systems*. Retrieved from https://www.schneier.com: https://www.schneier.com/blog/archives/2014/01/security_risks_9.html

117. *Secure360*. (2016, July 19). Retrieved from https://secure360.org/2016/07/why-are-cyber-criminals-always-a-step-ahead/

118. Sen, D. B. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Springer*, 49-69.

119. Sheard, J. (2010). Research Method . *Science Direct*, 429-452. Retrieved from https://www.sciencedirect.com: https://doi.org/10.1016/B978-0-08-102220-7.00018-2

120. Singh, A. (2019, June 12). *Device Authentication and Identity of Things (IDoT) for the Internet of Things (IoT)*. Retrieved from https://www.kuppingercole.com: https://www.kuppingercole.com/blog/singh/device-authentication-and-idot-for-iot

121. Smith, A. (2020, Feburary 16). *The Five Biggest Security Threats and Challenges for IoT*. Retrieved from https://dzone.com/articles/: https://dzone.com/articles/the-biggest-security-threats-and-challenges-for-io

122. Solutions, S. (n.d.). *Quantitative Research Approach*. Retrieved from https://www.statisticssolutions.com: https://www.statisticssolutions.com/quantitative-research-approach

123. Susanna. (2020). *How Secure is Your Small Business from Cyber Attacks?* Retrieved from https://www.timedoctor.com: https://www.timedoctor.com/blog/small-business-cyber-attacks/

124. Swinhoe, D. (2019, Feburary 13). *What is a man-in-the-middle attack*. Retrieved from https://www.csoonline.com: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html

125. Syed Kashan Ali Shah, W. M. (2020, October 8). *Smart Home Automation Using IOT and its Low Cost Implementation* . Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/344503210_Smart_Home_Automation_using_IoT_and_its_low_cost_implementation

126. Todd, S. T. (1995). Assessing IT Usage: The Role of Prior Experience. In S. T. Todd, *Assessing IT Usage: The Role of Prior Experience* (pp. 561-570). Management Information Systems Research Center, University of Minnesota.

127. Torriti, J. (2020). Appraising the Economics of Smart Meters: Costs and Benefits. *ResearchGate*.

128. Tsafantakis, M. (2019). *Organizational size and IT innovation adoption: A scrutiny of therelationship between size and e-Government maturity in Greekmunicipalities, through a citizen/service-oriented maturity model.* Retrieved from https://www.academia.edu: https://www.academia.edu/43641605/Organizational_size_and_IT_innovation_adoption_A_scrutiny_of_the_relationship_between_size_and_e_Government_maturity_in_Greek_municipalities_through_a_citizen_service_oriented_maturity_model

129. Tunggal, A. T. (2016, October). *What is vulnerability*. Retrieved from https://www.upguard.com/blog/vulnerability: https://www.upguard.com/blog/vulnerability

130. Tzafestas, S. G. (2018). Ethics and Law in the Internet of Things World. *MDPI*.

131. Venkatesh, V. (1998). User acceptance of information technology: A unified view. *ProQuest Dissertations and Theses*.

132. Viswanath Venkatesh, J. Y. (2012, March). Consumer Acceptance and Use of Information. *MIS Quarterly*, 157-178.

133. Viswanath Venkatesh, M. G. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425-478.

134. Warshaw, F. D. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. *Journal of Applied Social Psycology*, 1111-1132.

135. Watkins, A. C. (2012). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. In A. C. Watkins, *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* Kogan Page.

136. Wazir Zada Khan, M. K. (2019, September). *Advanced Persistance Threat Through Industrial IoT on Oil and Gas Industries*. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/335611873_Advanced_Persistent_Threats_Through_Industrial_IoT_On_Oil_And_Gas_Industry

137. Wiessberger, A. (2020, Feburary 20). *IEEE Communication Society*. Retrieved from https://techblog.comsoc.org: https://techblog.comsoc.org/2020/02/20/ciscos-annual-internet-report-2018-2023-forecasts-huge-growth-for-iot-and-m2m-tepid-growth-for-mobile/#:~:text=According%20to%20Cisco's%20newly%20renamed,to%2018.4%20billion%20in%202018.

138. Woken, M. D. (n.d.). *Advantage of Pilot Study*. Retrieved from https://www.uis.edu: https://www.uis.edu/ctl/wp-content/uploads/sites/76/2013/03/ctlths7.pdf

139. Wonjun Lee, S. S. (2018, April 4). *An Empirical Study of Consumer Adoption of Internet of Things Services.* Retrieved from https://core.ac.uk: https://core.ac.uk/download/pdf/228833731.pdf

140. Xi-Jun, L. H. (2015, February). *Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications*. Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/pii/S0167404814001229?via%3Dihub

141. Yap, J. Y. (1995). Information technology adoption by small business: Am empirical study. In J. P.-H. Karlheinz Kautz, *Diffusion and Adoption of Information Technology* (pp. 160-175). Oslo, Norway: Springer. Retrieved from https://link.springer.com: https://link.springer.com/content/pdf/10.1007/978-0-387-34982-4_12.pdf

142. Yaqoob, E. A. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, 10-16.

143. Yilmaz, K. (2013). Comparison of Quantitative and Qualitative Research Traditions: epistemological, theoretical, and methodological differences. *European Journal of Reserch Developmentb and Policy* , 311-325. Retrieved from https://doi.org/10.1111/ejed.12014

144. Yogesh K. Dwivedi, N. P. (2017, June 8). *Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model*. Retrieved from Springer: https://link.springer.com/article/10.1007/s10796-017-9774-y

145. Yu-Lin Zhao, J. T.-P.-L.-W.-C. (2020, July 28). *Development of IoT Technologies for Air Pollution Prevention and Improvement.* Retrieved from https://aaqr.org/articles: https://aaqr.org/articles/aaqr-20-05-oa-0255