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

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

ICFAI UNIVERSITY JHARKHAND
RANCHI
July, 2021

THESIS COMPLETION CERTIFICATE

This is to certify that the thesis entitled "**Barriers in Adoption of Internet of Things in Manufacturing Industries**" submitted by Mr. Gurvinder Singh, in Partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy is an original work carried out by him under our joint guidance. It is certified that the work has not been submitted anywhere else for the award of any other Degree or Diploma of this or any other university. We also certify that he complied with the plagiarism guidelines of the University.

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

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

DECLARATION OF AUTHORSHIP

I declare that this thesis titled "**Barriers in Adoption of Internet of Things in Manufacturing Industries**" submitted by me in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Management by the ICFAI University Jharkhand, Ranchi is my own work. It contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text. I further state that I complied with the plagiarism guidelines of the University, while preparing the thesis.

Gurvinder Singh
UID: 16JU11300010
1602, Neelkanth Residency,
Sector-46A, Seawoods, Nerul,
Navi Mumbai-400706
Date: 27th July 2021
Place: Navi Mumbai, Maharashtra

PLARIARISM REPORT

Ouriginal

Document Information

Analyzed document	Thesis Gurvinder final for Plagarism test.docx (D122822566)
Submitted	2021-12-17T06:16:00.0000000
Submitted by	RUMNA BHATTACHARYYA
Submitter email	rumna.b@iujharkhand.edu.in
Similarity	2%
Analysis address	rumna.b.iujhar@analysis.urkund.com

Sources included in the report

J	URL: 3182246e-2771-4273-863f-7e4a7c62acb8 Fetched: 2018-08-16T14:29:08.0000000	9
W	URL: https://www.iotworldtoday.com/2016/04/20/top-10-reasons-people-aren-t-embracing-iot/ Fetched: 2019-10-24T23:57:21.3530000	3
J	URL: b68ad25b-e08b-4be6-9458-d4904d880a3f Fetched: 2018-08-16T14:29:12.0000000	1

ACKNOWLEDGEMENT

First, I would like to dedicate this work to the Almighty who gave me the strength, wisdom, and knowledge to work in this area and complete a major milestone of my life. I would also like to thank my parents whose consistent efforts enabled me for this highest disagree in education.

I would like to thank ICFAI University, Jharkhand; for allowing me to pursue research in the topic of my interest. I am very grateful to Prof. ORS Rao who gave me directions to streamline the topic of study and supported me throughout the journey. Sir, your suggestions and mentoring always showed the path to me to get out of any difficult situation. I am very grateful to my supervisor Dr.Tarak Nath Paul and Co-supervisor Dr. Sushil Kumar Pare who continuously pushed me to think out of the box to get the desired results. Their supervision gave me the confidence to bring professional research to the table which will benefit future scholars and industry. I am also thankful to Dr. Yogesh Funde, assistant professor at NMIMS who helped me in designing research methodology. Special gratitude to Dr. B M Singh, Dr. K K Nag, Dr Hari Haran, and Dr.S C Swain for sharing their vast and enriching experience during coursework and progress review sessions to keep my study on the right track. I am indebted to the Research Board of the ICFAI University, Jharkhand, headed by Honourable Vice-Chancellor Prof. ORS Rao and its members Dr. M Rajkumar, Dr. Barik Bhagabat, Dr. Dilip Kumar, Dr.Subrato Kumar Dey and Dr. Pallavi Kumari who contributed in enabling a quality research by way of their suggestions in the various half-yearly progress reviews & regular reviews with their critical evaluations. I am very thankful to Dr. Rumna Bhattacharya who was very prompt and helpful during administrative challenges.

I am thankful to my loving wife (Ishmeet) who realized the importance of this dream for me and encouraged me to start it. You always supported me to find time for this study in my busy schedule

and sacrificed your time. Without you standing by me and taking many responsibilities of mine, this journey would not have started and completed. Your contribution to success is equal. I am thankful to you from the bottom of my heart. My daughters, Harbaani and Joggeet, the excitement in your eyes to hold my Ph.D. degree always gave me the strength to give sincere efforts to complete the study in time.

I would also like to thank my school and college teachers and mentors who helped me attain the highest education degree. Special thanks to my school principal, Surender Kaur who has been an inspiration for many. Although we have not met for years, your learnings and motivational speeches have a significant role in this success.

Finally, my heartfelt gratitude to my classmates who supported and guided me to achieve different milestones of this study.

(Gurvinder Singh)

Date: 27th June 2021

Place: Navi Mumbai, Maharashtra

ABSTRACT

The research topic of this study is the factors that can influence the adoption of IoT in manufacturing companies in and around Mumbai. The Internet of Things (IoT) is the developing network of connected smart devices using internet protocols. Its gaining popularity in different industries due to many advantages. However, there are several reservations in the adoption like any new technology face at the initial stage.

The literature study on the adoption of technologies and different technology adoption models proposed by several authors explored many reasons which hamper the adoption of technologies. Several authors have explored that adoption of the IoT will be delayed if security issues are not addressed. Some authors have argued that users often ignore security and privacy over convenience. Similarly, authors have revealed other factors that can influence the adoption of technologies like performance expectancy, effort expectancy, facilitating conditions, social influence, and competition, etc. The authors have addressed these factors and presented findings that support the influence of these factors on the adoption of technologies. Some literature does not support the influence.

As IoT has several benefits for the manufacturing industry, the purpose of this study is to explore important factors that can influence adoption. These factors are studied by different authors for different technologies adoption and this research will give a unified view for manufacturing organisations. This research was constructed to explore important factors that can influence the adoption of IoT in manufacturing industries in and around Mumbai. The Unified Theory of Acceptance and Use of Technology (UTAUT) was used to define three constructs for this study

that are performance expectancy, effort expectancy, and facilitating conditions. Security awareness was added as an additional construct to fulfil the requirement of this study. Further, the impact of organization size on the relationship between each factor and adoption of IoT is checked using the large, medium, and small size organisation as moderators.

It is a quantitative non-experimental correlational study to measure the influence. The target group of the research was the owners and senior management who are running large, small, and medium size manufacturing enterprises in and around Mumbai. The source of contact details was the Ministry of Micro Small and Medium Enterprises (MSME) office in Delhi. Telephonic and face to face survey was the mode of collecting data. The research method chosen for this study was a quantitative, non-experimental, correlational study using regression as the form of data analysis. Multiple regression was used as the statistical analysis to perform hypothesis testing to answer the research questions. The organisation size is used as a moderator to check its influence on the relationship between independent variables and dependent variable.

At last, the study concluded that security awareness, performance expectancy, effort expectancy, and facilitating conditions are statistically significant and influence the adoption of IoT. The organisation size also moderates the relationship between each factor and the adoption of IoT. The further analysis explored that small and medium size organisation has significant influence while large size organisations have moderate influence.

The study has opened opportunities for further research like exploring security awareness in detail which is one of the important factors in this era due to increasing cybercrime incidents. Further, the study has given a model which can be used for different industries to understand the reasons depleting adoption of IoT. The study also gives enormous benefits to IoT service providers, government and regulatory bodies, and education institutes.

TABLE OF CONTENTS

PART 1

PART - 2

PART 3

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

Acronym	Full Form
IoT	Internet of Thing
IIoT	Industrial Internet of Things
SA	Security Awareness
PE	Performance Expectancy
EE	Effort Expectancy
FC	Facilitating Conditions
UTAUT	Unified Theory of
TAM	Technology Acceptance Model
IDT	Innovation Diffusion Theory
TRA	Theory of Reasoned Action
TPB	Theory of Planned Behavior
C-TAM-TPB	Combined-TAM-TPB model
MM	Motivational Model
RFID	Radio Frequency Identification
M2M	Machine to Machine
NFC	Near Field Communication
IDC	International Data Corporation
ICT	Information and Communication Technology
MiTM	Man in The Middle
DoS	Denial of Service
DDoS	Distributed Denial of Service

XMPP	Extensible Messaging and Presence Protocol
MQTT	Message Queuing Telemetry Transport
CoAP	Constrained Application Protocol
DSS	Decision Support System
AMqP	Advanced Message Queuing Protocol
HTTP	Hypertext Transfer Protocol
VPN	Virtual Private Network
DNS	Domain Name Service
APT	Advanced Persistent Threat
PII	Personally, Identifiable Information
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SSL	Secure Sockets Layer
WAF	Web Application Firewall
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DCCP	Datagram Congestion Control Protocol
SCTP	Stream Control Transmission Protocol
RSVP	Resource Reservation Protocol
DTLS	Datagram Transport Layer Security
TLS	Transport Layer Security
SOAR	Security Orchestration, Automation, and Response
IETF	The Internet Engineering Task Force

ICANN	Internet Corporation for Assigned Names and Numbers
RIR	Regional Internet Registry
ISOC	Internet Society
IEEE	Institute of Electrical and Electronics Engineers
IGF	Internet Governance Forum
W3C	World Wide Web Consortium
MPCU	Model of Personal Computer Utilization
VIF	Variation Inflation Factor
MSME	Micro Small and Medium Enterprises

CHAPTER 1:

INTRODUCTION

CHAPTER 1: INTRODUCTION

1.1 Overview

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 model, 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 consumer intention to adopt the 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 organisation on these factors.

1.1.1 Security Awareness

Security Awareness explains the consumers' understanding of security threats that occurs due to IoT and related devices. It explains user understanding of security threats like malware, phishing, ransomware attacks etc. It also covers the users understanding of the impact due to security threats like data loss, privacy loss, remotely hacking of machines and loss of reputation. Security Awareness construct is used by Allen A. Harper in his study along with other constructs from UTAUT. By expanding the UTAUT to cover the construct of security awareness, the model may be useful for understanding other areas of technology adoption (Harper, 2016).

1.1.2 Performance Expectancy

Performance Expectancy is defined as the consumers' expectation that the use of IoT will improve performance. It explains users' expectations on reduce time of production, improve the quality of products, reduce effort of production etc. Performance expectancy is drawn from other constructs, including the perceived usefulness of the Technology Acceptance Model (TAM) (Davis, 1993). Performance Expectancy was found to be the strongest predictor of behavioural intention to use technology (Venkatesh& Thong, 2012).

1.1.3 Effort Expectancy

Effort Expectancy is defined as the measure of the perceived ease of use of the technology like can technology be integrated with existing technology in use, is it easy to learn the technology or train staff on it, can new technology be learned easily etc. Effort Expectancy is also drawn from other constructs of other models, such as perceived ease of use, of the Technology Acceptance Model (TAM) (Davis, 1993).

1.1.4 Facilitating Conditions

Facilitating Conditions are defined as a collection of perceived infrastructures the user believes exists, to facilitate the use of the technology like availability of skilled resources who can deploy and use the technology, sufficient knowledge is available to use and troubleshoot etc. As with the other constructs, the Facilitating Condition construct is derived from other models, including the innovation diffusion theory (IDT) of Moore and Benbasat (1991) .

There are many pieces of literature on the IoT which addressed substantial security issues with IoT that are unresolved. Although the technology of the IoT has great potential, security issues continue to plague the technology (Jun, 2015). User data privacy and security are major concerns. In the area of wireless, data transfer integrity is at risk. Several authors pointed out that the privacy of sensitive data collected by IoT devices is a major issue.

As will be further highlighted in the literature review, there is an increasing frequency of articles addressing the security issues of the IoT (Harper, 2016). However, it is still not qualified that awareness of security threats is the primary reason for the acceptance of IoT or other drivers are contributing to the decision-making of adoption of IoT.

1.2 Motivation of the Study

The IoT is the use of smart sensors and actuators to enhance manufacturing and industrial processes that are also known as the industrial internet or Industry 4.0. IoT leverages the power of smart machines and real-time analytics to take advantage of the data that 'dumb machines' have produced in industrial settings for years. The driving philosophy behind IoT is that smart machines are not only better than humans at capturing and analysing data in real-time, but they are also better at communicating important information that can be used to drive business decisions faster and more accurately (Rouse, 2020).

Connected sensors and actuators enable companies to pick up on inefficiencies and problems sooner and save time and money in addition to supporting business intelligence (BI) efforts. The IoT has a prospective for quality control, sustainability, supply chain traceability, and overall supply chain efficiency. In an industrial setting, IoT is key to processes such as predictive maintenance, enhanced field service, energy management, and asset tracking (Rouse, industrial internet of things (IIoT), 2020).

The IoT is moving full steam ahead undoubtfully. Both Cisco and McKinsey predict that the IoT is capable to generate business of more than $10 trillion in the coming decade. Cisco predicts the market could be worth $14.4 trillion by 2025.

The advantages of IoT are very well accepted and known. However, there are several articles and white papers that keep discovering the security issues associated with IoT which is a primary concern for the industry to not accept. Data protection and security concerns are the fundamental reasons for the industry to not adopt it. In the post-Snowden era, data privacy remains a potential concern for the IoT. And because IoT devices can potentially harvest enormous amounts of data,

security breaches can be especially dangerous (Buntz, 2016). Companies designing industrial IoT applications can face significant challenges because many industrial devices were historically designed to be secured by isolation. Making these systems talk to external networks, securely can be a tricky proposition (Buntz, 2016).

As the study is for technology adoption, it is important to understand other factors which can impact the adoption of IoT. Several theoretical models have been perused to seek factors that influence behavioural intentions to use technology to manage user behaviour. Models scanned include the Theory of Reasoned Action (TRA) (Ajzen, 1975); the Theory of Planned Behaviour (TPB) (Ajzen, 1991), the Technology Acceptance Model (TAM) (Davis, 1993), the Combined-TAM-TPB model (C-TAM-TPB) (Todd, 1995), the Motivational Model (MM) (Warshaw, 1992), the Innovation Diffusion Theory (IDT) (Rogers, 2019) and others. Combinations of the listed models have been applied as theoretical models in some situations while in others and these models have been extended with additional factors too. In 2003, for example, Venkatesh et al. unified eight of these models and arrived at the UTAUT model which can explain 70% of the variance in user intention. The results of that pragmatic study demonstrated that the UTAUT model is the most effective model for analysing technology acceptance (Chao, 2019). The UTAUT model consists of six main constructs, namely performance expectancy, effort expectancy, social influence, facilitating conditions, behavioural intention to use the system, and usage behaviour.

This study is constructed with a motivation to build a combination of the UTAUT model and user's awareness of security constructs. The study predominantly focuses on the three constructs of UTAUT - Performance Expectancy, Effort Expectancy, and Facilitating Conditions. The fourth construct, Security Awareness is added. The selected construct will explore if awareness of security

threats is the reason for the slow adoption of IoT or other factors are also responsible for it. The study will also reveal the impact of the size of the company on all constructs.

1.3 Scope of the Study

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 play a significant role in the adoption of 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).

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 restricting the adoption of IoT in the manufacturing industry in and around Mumbai. The study analyses, security awareness, performance expectancy, effort expectancy, and facilitating conditions. The study will explore the impact of large, medium, and small-size organisations on these constructs. The resulting report will help IoT vendors, service providers, and business managers increase IoT adoption.

1.4 Relevance of the Topic

The purpose of this non-experimental correlation study is to measure the correlation, if any, of security awareness, performance expectancy, effort expectancy, facilitating conditions, and organisation size on the consumer intention to adopt the IoT. An understanding of this relationship will become 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 secure 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 above factors, the solutions are required to cater to the need of specific size of 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 consumer intention of adoption of the IoT, changes will be made sooner to increase the adoption rate.

1.5 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 consumer intention to adopt IoT. The size of the organization will be used as a moderator to check its impact on the dependent variable.

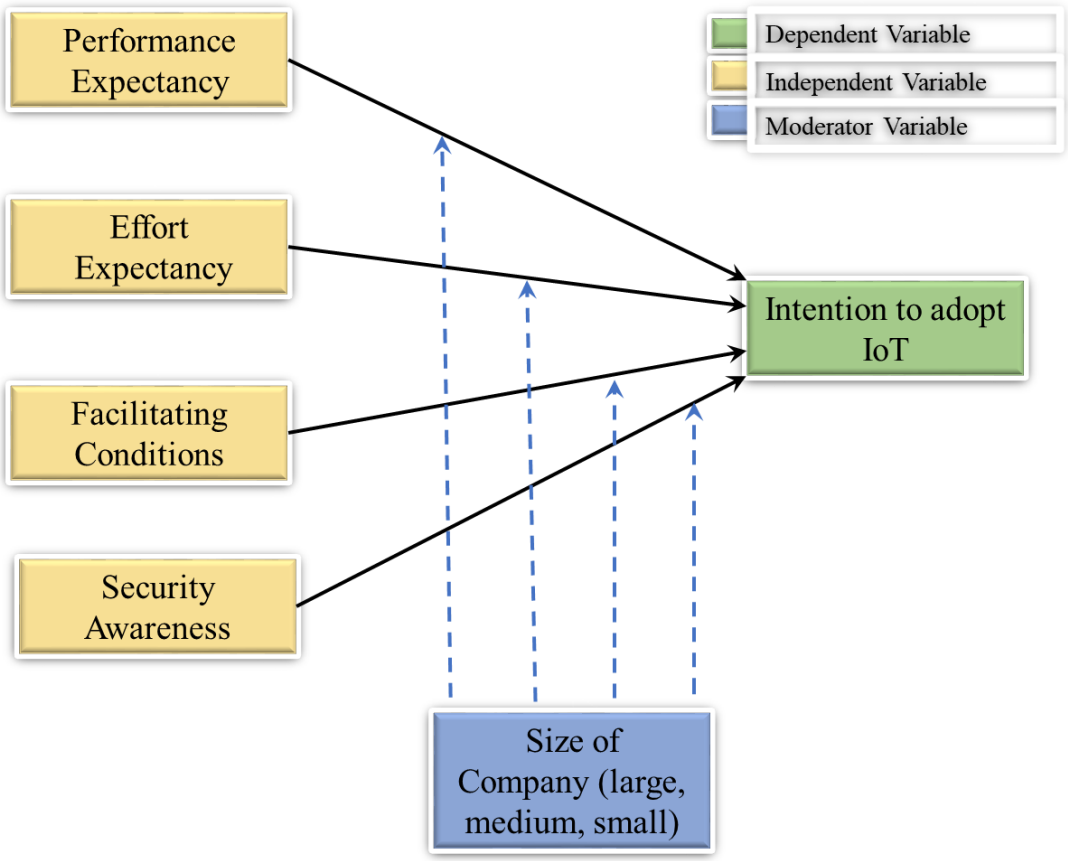

Figure 1-1: Framework of Study

1.6 Research Questions

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 will support the research objective. The primary research question addresses the research topic: the impact of security awareness on the consumer intention to adopt IoT. The secondary research questions will attempt to identify the other factors in addition to security awareness that affects the consumer intention. The primary and secondary research questions are as follow:

1.6.1 Research Question 1

The primary research question for this topic is: to what extent, if any, does a consumer's security awareness influence the adopt the IoT? The following two hypotheses apply to this question:

$H_{1.0}$: 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

The secondary research questions for this topic address the other constructs of the UTAUT (Venkatesh & Thong, 2012) and allow for hypothesis testing and an analysis of each coefficient of the extended model:

1.6.2 Research Question 2

To what extent, if any, does Performance Expectancy influence consumer intention to adopt the IoT? The following two hypotheses apply to this question:

$H_{2.0}$: 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.

1.6.3 Research Question 3

To what extent, if any, does Effort Expectancy influence consumer intention to adopt the IoT? The following two hypotheses apply to this question:

$H_{3.0}$: 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.

1.6.4 Research Question 4

To what extent, if any, does Facilitating Conditions influence consumer intention to adopt the IoT? The following two hypotheses apply to this question:

$H_{4.0}$: 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.

The above research questions and associated hypothesis are summarised in the table.

Research Questions	Hypothesis	Description
Does consumer security awareness influence consumer intention to adopt IoT?	**H1.0:** Security Awareness influences the consumer intention to adopt the IoT in manufacturing companies in and around Mumbai	To what extent, if any, consumer security awareness influence adoption of Internet of Things and does organisation size moderates this relationship. If yes, which size of the organisations moderates this relationship.
Does consumer security awareness with moderator Organisation Size influence consumer intention to adopt IoT?	**H1.1:** The Organisation Size moderates relationship between Security Awareness and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai	
Does performance expectancy influence consumer intention to adopt IoT?	**H2.0:** Performance Expectancy influences consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.	To what extent, if any, does performance expectancy influence adoption of Internet of Things and does organisation size moderates this relationship. If yes, which size of the organisations moderates this relationship.
Does performance expectancy with moderator Organisation Size influence consumer intention to adopt IoT?	**H2.1:** The Organisation Size moderates the relationship between Performance Expectancy and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.	
Does effort expectancy influence adoption of IoT?	**H3.0:** Effort Expectancy influences consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.	To what extent, if any, does effort expectancy influence adoption of Internet of Things and does organisation size moderates this
Does effort expectancy with moderator	**H3.1:** The Organisation Size moderates the relationship between	

Organisation Size influence adoption of IoT?	Effort Expectancy and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.	relationship. If yes, which size of the organisations moderates this relationship.
Does facilitating conditions influence adoption of IoT? Does facilitating conditions with moderator Organisation Size influence adoption of IoT?	**H4.0:** Facilitating Conditions influence consumer intention to adopt the IoT in manufacturing companies in and around Mumbai. **H4.1:** The Organisation Size moderates the relationship between Facilitating Conditions and consumer intention to adopt the IoT in manufacturing companies in and around Mumbai.	To what extent, if any, does Facilitating Conditions influence adoption of Internet of Things and does organisation size moderates this relationship. If yes, which size of the organisations moderates this relationship.

Table 1-1: Summary of questions and hypothesis

1.7 Significance of Study

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 IoT study of Allen A. Harper (Harper, 2016) will be followed as an example.

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.

1.8 Assumptions and Limitations

1.8.1 Assumptions

The following are the assumptions made in this study:

Appropriateness of UTAUT model for this study

Since the UTAUT is a widely used model for measuring the adoption of technologies, it is assumed that it is suitable for this study too. Further, it is assumed that the UTAUT model can be extended as done in other studies (Harper, 2016). In this study security awareness is the construct which is added along with UTAUT constructs. Also, one of the constructs used in UTAUT, social influence, is not considered in this study. It is assumed that social influence has no impact on the adoption of technology for industrial purposes. This construct is more suitable for personally used technology like mobile phones.

The honesty of participants to answer survey questions

It is not possible to measure the honesty of the users hence, it is assumed that participants will answer to the best of their knowledge and honest in answering the survey questions. It is also assumed that the target group of the research who is the owner and senior management of large, medium and small size manufacturing enterprises are the best participants to answer the survey questions. The outliers and incomplete data will be removed to maintain data consistency.

1.8.2 Limitations

Limitations of researcher

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.

Limitation of generalization

Sampling is done in a random (probabilistic) manner, or a purposive (non-probabilistic) manner (Hedges, 2013). The main difference between the two is the ability to extend the results to a broader population, which is called generalizability (Yilmaz, 2013). To generalize the results to the broader population, a study with a probabilistic sample is chosen over the alternative, although it is rarely achievable in practice (Hedges, 2013). The Surveys were conducted face to face and through telephone and senior staff, entrepreneurs, and IT heads participated in the survey. The contact

details of these people are taken from reputed internet sites and through personal contacts. As these people were chosen randomly from the database, the generalization of the study may be affected.

1.9 Summary

The chapter covers overview of the IoT. The four main constructs were also discussed thoroughly that are important for this study. Thereafter, motivation and scope of the study is explained. The framework of the study is also provided to understand different constructs involved. The four research questions were explained in detail along with associated hypotheses. The chapter was ended with explanation of significance, assumptions, and limitations.

CHAPTER 2:
REVIEW OF LITERATURE

CHAPTER 2: REVIEW OF LITERATURE

2.1 What is Internet of Things

Technology is advancing with the speed of light. The enhancement in requirements from connectivity at any time and any place to connectivity for anything has given birth to IoT. The internet on mobile and other mobile devices keeps us connected anytime and at any place. However, the requirement is now to connect non-mobile things with other non-mobile and/or mobile things which can be fulfilled by IoT. These “things” of the real world shall seamlessly integrate into the virtual world, enabling anytime, anywhere, and anything connectivity. In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Cisco forecasts that this figure is expected to 29.3 billion by 2023 as the number of more smart devices per person increases. The report also anticipates that IoT will spread to 50% of all networked devices through machine-to-machine (M2M) technology and that the internet will reach 5.3 billion people, compared to 3.9 billion in 2018 (Wiessberger, 2020).

The Internet of Things refers to the networking of physical objects with unique identifiers and embedded with sensors. These devices can collect information from other devices and/or transmit information about the devices without human-to-human or human-to-computer interaction. The data collected from these devices can then be structured, analysed to optimize products, services, and operations.

The Wikipedia describes Internet of Things as The Internet of Objects, refers to a wireless network between objects; usually, the network will be wireless and self-configuring, such as household appliances.

By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves (RFIC, n.d.).

2.2 Benefits of IoT

IoT brings in several benefits for business, consumers, and society like reduced production cost through automation, increase efficiency of production and distribution, high-quality products for customers at a lesser cost, improvisation of lifestyle through the smart city etc. The boon for IoT are countless (Hittinger, 2019).

These benefits of IoT cab be classified into three C's of IoT.

Communication

IoT-enabled devices communicate information to people and systems, such as state and health of equipment (e.g. It's on or off, charged, full or empty) and data from sensors that can monitor a person's vital signs like pulse rate, oxygen level, blood pressure level etc. In most cases, we didn't have access to this information before, or it was collected manually and infrequently. For example, an IoT-enabled HVAC system can report if its air filter is clean and functioning properly. Almost every company has a class of assets it could track. GPS-enabled assets can communicate their current location and movement. Location is important for items that move, such as trucks, but it's also applicable for locating items and people within an organization. In the healthcare industry, IoT can help a hospital track the location of everything from wheelchairs to cardiac defibrillators to surgeons. In the transportation industry, a business can deliver real-time tracking and condition of

parcels and pallets. For example, Maersk can use sensors to track the location of a refrigerated shipping container and its current temperature (Morley, 2018).

Control and Automation

In a connected world, a business will have visibility into a device's condition. In many cases, a business or consumer will also be able to remotely control a device. For example, a business can remotely turn on or shut down a specific piece of equipment or adjust the temperature in a climate-controlled environment. Meanwhile, a consumer uses IoT to unlock their car or start the washing machine. Once a performance baseline has been established, a process can send alerts for anomalies and possibly deliver an automated response. For example, if the brake pads on a truck are about to fail, it can prompt the company to take the vehicle out of service and automatically schedule maintenance (Chaudhury, 2018).

Cost Savings

Many companies will adopt IoT to save money. Measurement provides actual performance data and equipment health, instead of just estimates. Businesses, particularly industrial companies, lose money when equipment fails. With new sensor information, IoT can help a company save money by minimizing equipment failure and allowing the business to perform planned maintenance. Sensors can also measure items, such as driving behaviour and speed, to reduce fuel expense and wear and tear on consumables. New smart meters in homes and businesses can also provide data that helps people understand energy consumption and opportunities for cost savings (Torriti, 2020).

2.3 Application of IoT

The popularity of IoT has increased drastically in the last few years. In one of the data analyses done on Google, Twitter, and LinkedIn in the year 2015, it was concluded people are curious to

know about IoT technology and the benefits they can achieve from it. The smart home, smart city, and smart grid have a maximum search on Google search engine.

2.3.1 Smart Home

Wireless Home Automation system (WHAS) using IoT is a system that uses computers or mobile devices to manage many home functions and features like a microwave, refrigerator, air conditioner, etc. These devices can be connected from anywhere through the internet. An automated home is sometimes called a smart home. It is meant to save electric power and human energy. Imagine you can set room temperature through mobile while you leave the office, or your coffee machine readies a cup of coffee when you reach home from the office. Smart home automation systems are defined as implementing the system within the home environment to facilitate its customers by providing comfort, convenience, and energy efficiency (Shah, 2020).

Smart Home stands out, ranking as the highest internet of things application on all measured channels. More than 60,000 people currently search for the term “Smart Home” each month. This is not a surprise. The IoT Analytics company database for Smart Home includes 256 companies and start-ups. More companies are active in the smart home than any other application in the field of IoT. The total amount of funding for Smart Home start-ups currently exceeds $2.5bn. This list includes prominent start-up names such as Nest or AlertMe as well as several multinational corporations like Philips, Haier, or Belkin.

2.3.2 Smart City

The habitation of the high population in urban cities has increased resource utilization drastically in the last couple of years. In this situation, the expansion of IT and automation are expanding the potential of infrastructure across the world. Solutions for sustainable power distribution, efficient traffic systems, and efficient, intelligent buildings are becoming more flexible and adaptable to new conditions.

Converting cities into Smart cities through IoT spans a wide variety of use cases, traffic management, water distribution, waste management, urban security, and environmental monitoring. The Smart City solutions promise to improve the standard of living of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer. The UN predicts that by 2050, the world's urban population is likely to double and reach the point of nearly 6.7 million people. As the number of urban residents grows, cities face new opportunities and challenges. To prevent environmental deterioration, avoid sanitation problems, mitigate traffic congestion, and thwart urban crime, municipalities turn to the Internet of Things (IoT) (Grizhnevich, 2018).

2.3.3 Control Air Pollution

The increasing air pollution is the biggest problem for any government of urban cities. Using smart sensors and data analysis air pollution for a city can be reduced to a certain extent. The factors which are contributing to the increasing air pollution can be controlled. Imagine if you are getting information about pollution levels on your mobile of the area where you are jogging in the morning. You can take a better way to intake healthy air. The realization of such a service requires that air

quality and pollution sensors be deployed across the city and that the sensor data be made publicly available to citizens. The IoT-based air quality monitoring platform could perform online monitoring and real-time response and realizes 24 hours of air condition monitoring throughout the day and proposed the method of using intelligent sensor networks for monitoring. It was also proved that the air quality has a great impact on human health with monitoring indoor air conditions (Zhao, 2020).

2.3.4 Waste Management

Waste management is a primary issue for many modern cities. The solution for this issue needs a deep study of technologies and automation through IOT for economic and ecological advantages. For instance, the use of intelligent waste containers which detect capacity and route to optimize truck utilization is used to carry waste to reduce cost and efficiently manage the waste. Well-organized waste collection is considered a fundamental service for smart cities. Internet of Things can be applied both in intelligent transport system and smart cities creating an advanced platform for novel applications. Surveillance systems can be used for high Quality of Service (QoS) in waste collection. Precisely, IoT components like RFIDs, sensors, cameras, and actuators are incorporated into ITS and surveillance systems for efficient waste collection (Medvedev, 2015).

2.3.5 Noise Monitoring

Noise can be seen as a form of acoustic pollution as much as carbon oxide (CO) is for air. The city authorities have already issued specific laws to reduce the amount of noise in the city at specific hours. An urban IoT can offer a noise monitoring service to measure the amount of noise produced

at any given hour in the places that adopt the service. Therefore, noise pollution must be a severe world public health challenge and should be monitored not only inside buildings but also in outside for enhanced living environments in smart cities. Noise real-time monitoring can be possible with IoT bases systems which allow the detection of unhealthy situations and to notify respective authorities to take interventions to decrease the sound levels quickly (Marques, 2019). Besides controlling noise pollution, such a service can also be used to enforce public security, employing sound detection algorithms that can recognize, for instance, the noise of glass crashes or brawls. This service can hence improve both the quiet of the nights in the city and the security for the public. On another side, the installation of sound detectors or environmental microphones is quite controversial, because of the obvious privacy concerns for this type of monitoring.

2.3.6 Traffic Congestion

Monitoring traffic congestion in urban cities is another service offered by IoT. It is on the same line of air quality control and noise monitoring. The camera-based traffic monitoring systems are already available and deployed in many cities to monitor traffic congestion and the speed of vehicles. However, low-power widespread communication can provide a denser source of information. Effective traffic monitoring may be realized by increasing the density of sensing capabilities and GPS installed on modern vehicles. A solution adopting a combination of air quality and acoustic sensors along a given road can be the most effective solution to discipline traffic and to send officers where needed, plan the route to reach the office, or better schedule a shopping trip to the shopping mall. As per Victoria transport policy institute urban mobility report 5.5 billion hours and 2.9 billion gallon of fuel waste in Urban cities of Unites States due to traffic Jams. Several solutions were experimented and failed to deliver desired results. However, IoT based solutions

could resolve many challenges and found to have potential to solve traffic jams in United States (Chowdhury, 2016).

2.3.7 City Energy Consumption

The IoT for urban cities also provides a service to monitor the energy distribution and consumption of the city. It enables authorities and citizens to get a detailed view of the amount of energy required by the different services like lighting at public places, transportation, traffic signals, control cameras, heating/ cooling of public buildings, and so on. The benefit is, this will make it possible to identify the main energy consumption sources and to set priorities. By using only smart lighting systems, authorities can realize a saving of electricity. This service can optimize the streetlamp intensity according to the time of the day, the weather condition, and the presence of people. To obtain such a service, power draw monitoring devices must be integrated with the power grid in the city. In addition, it will also be possible to enhance these services with active functionalities to control local power production structures (e.g., photovoltaic panels). The government has taken several actions to reduce the consumption of electricity for streetlights like HPS (High-Pressure Sodium) lamps are replaced with LED (Light Emitted Diodes). However, there is a further need to reduce consumption and IoT solutions can make it possible (Dizon, 2021).

2.3.8 Smart Parking

The smart IoT-enabled parking service is based on road sensors and intelligent displays that direct motorists along the best path for parking in the city. The benefits deriving from this service are manifold: faster time to locate a parking slot means fewer CO emissions from the car, lesser

traffic congestion, and reduced noise pollution. The smart parking service can be directly integrated with the urban IoT infrastructure. By using technologies such as Radio Frequency Identifiers (RFID) or Near Field Communication (NFC), it is possible to realize an electronic verification system of parking permits in slots reserved for residents or disabled, thus offering a better service to citizens that can legitimately use those slots and an efficient tool to quickly spot violations.

2.3.9 Automation of Public Buildings

Another important application of IoT technologies is the monitoring of the energy consumption and temperature control for public buildings like schools, administration offices, and museums through different types of sensors. By controlling light, humidity, temperature, and other factors for human comfort, indeed, it will have a positive return in terms of productivity, while reducing the costs.

From the analysis of the services described, it emerges that Smart cities need a centralized architecture where the dense set of peripherals are transmitting and receiving data that is delivered to a centralized location for processing and analysis.

2.3.10 Smart Grids

A smart grid is an energy delivery consumer-driven, iterative system. It relies on bi-directional communication to constantly adapt and tune the delivery of energy. A smart grid includes many components, including a broad range of sophisticated sensors. These components are constantly assessing the state of the grid, the availability of power flowing into the grid, and the demand on

the grid. They are also capable of collecting a vast amount of this information over time, to determine what "behaviours" can be changed to optimize energy delivery.

The objective of the smart grid is to deliver the right amount of energy at the right place and at right time. The most important concept in the delivery of electricity is peak demand. For example, when it is really hot outside, everyone runs their air conditioner. They also go to the refrigerator to grab a drink. Since it's so hot outside, they may as well get something done inside, so why not throw a load of laundry in the washing machine and turn on the TV? All of this spikes the demand challenging utilities and to meet demand, it is a great cost. IoT has become an enabling technology to provide innovative solutions to overcome the challenges in the power grid system. IoT-enabled sensors are used extensively in the power grid system to share their useful information through internet and web applications, enabling improved grid management (Khan, 2020).

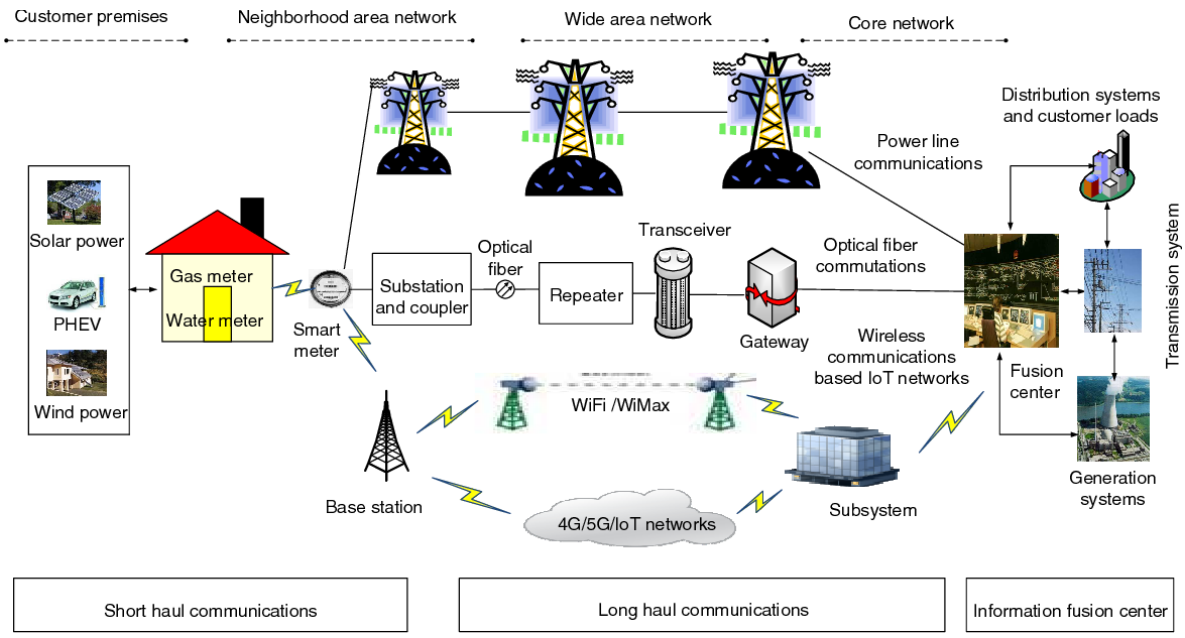

Figure 2-1:Various communication protocols of a smart grid (Rana et al., 2017)

The first key step towards a smart grid that makes the IoT real is the mass deployment of smart meters. First, meters need to report energy consumption information from houses and buildings back to the utilities. Second, the meter needs to deliver useful power consumption information into the home through an in-home display or a gateway. This information allows consumers to adopt energy behaviour and lower utility bills.

From production to consumption, the substation is the key piece of grid equipment that establishes the link between utilities and homes and building premises. A substation transforms voltage, drives the flow of power, isolates, and reroutes the power path as needed, manages and coordinates distributed energy sources from solar to wind, and deals with power outages and recovery. The ability to dynamically locate, map, monitor and control the substation at the city, state, or country level is one of the key goals of an automated distribution to ensure better grid operation.

2.3.11 Connected Cars

The concept of the connected car is coming up slowly. The car customers are now looking for vehicles that are technology friendly. Although science friction long predicted connected and self-driving vehicles concept. However, advancement in this area needs to go long. The big technology giants like Google, Microsoft, and Apple have announced connected car platforms. Now it's on car manufacturers to present next-generation internet-connected cars soon and make life safer and more convenient for motorists. Future capabilities in this industry are likely to include:

Integration with Home Networks

It is widely predicted that vehicles will be connected with buildings and perhaps switching on lights, heating, or air conditioning systems. Volkswagen also believes it will be important for homes

to exchange information with the vehicle while it is parked outside; transferring downloaded music, media, and journey plans while checking vehicle's status – for example, temperature or oil level – mileage information and journey statistics.

Data Exchange with Insurers, Manufacturers, and Third Parties

Telemetric systems will store information within the vehicle, the so-called "black box". Two-way communication will enable insurers to review usage remotely in real-time, manufacturers to monitor and refine performance, and third-party subscription services to record and analyse travel patterns.

Diagnostics and Vehicle Health Reports

Connected cars will be able to contact mechanics and garages directly with diagnostics issues, keeping performance parameters under review, and informing the driver earlier at any sign of trouble.

In-vehicle Wi-Fi Hotspot

Whether supplied by the manufacturer or retrofitted, systems are already available to provide local Wi-Fi for passengers' handheld and wireless devices. To meet high competition in the car industry, it seems likely that Wi-Fi in cars will become a standardized feature.

Social Media tie-ins

The automotive industry has found social media for marketing a very effective method. It helps them to engage customers with the brand. The development of the car into a location-aware, internet-connected device opens new possibilities, from simple automated check-ins and status updates to positioning-based engagement.

Payment Integration

With the right account setup, cars with wireless connectivity will be able to pay automatically for incidental, driving-related costs such as road tolls, parking, and, potentially, fuel.

Streaming of Music and Video on Demand

Entertainment will no longer be restricted to physical discs and even mp3 players. Access to on-demand media will give drivers and passengers countless songs, movies, TV shows, and games on the road.

Localized Information and Advertising

There is the potential for motorists to benefit from relevant, highly localized information, warnings, and offers, from improved weather and traffic reports to short-term discounts at nearby outlets, fuel price information, and parking availability.

Police Warnings and Location

To improve safety, vehicle connectivity could enable Police and other authorities to issue targeted warnings – whether based upon a defined location or direct to individual vehicles – while also empowering them to locate a connected car for security or recovery reasons.

Real-time Traffic and Incident Alerts

Cars will be increasingly warned of traffic and incidents ahead, prompting them to slow down or change lanes or routes, and adjusting journey time predictions as appropriate. As this becomes more sophisticated, signals from other cars already in traffic will begin to inform in-vehicle navigation systems in real-time.

The vehicle's evolving ability to aggregate, interpret and share information will make driving safer, easier, and more comfortable. Communication between vehicles will enable traffic to flow more easily through junctions, and for cars to maintain safer braking distances when traffic ahead slows down. Potentially it would reduce road accidents.

2.3.12 Smart Retail

The retail industry is increasingly coming in direct contact with consumers through IoT-related technology and innovation. Leading retailers are already developing strategies and plan to take advantage of IoT-related technologies. As retailers continue to digitize the consumer experience the spending on it will grow significantly. Worldwide spending on digital transformation will reach $2.3 trillion in 2023, more than half of all ICT spending, according to a new IDC spending guide (IDC, 2019). New technologies are keeping customers connect to brands and give the right retail experience and the right time to inspire lifelong brand loyalty. IoT data harvested from smartphones, wearables, sensors, and other devices will provide significant new insights and opportunities. Paired with cognitive computing, this IoT-generated data will assist retailers in understanding and responding to the disrupted landscape and changing customer expectations. Retailers that want to take advantage of the Internet of Things will innovate in four areas:

Enhanced Customer Experience

Increasingly, customers expect personalized service based on their shopping histories and value a one-on-one relationship with a brand. Combining data from in-store IoT devices with customer shopping history, retailers can create a single view of each customer, find patterns and deliver a more relevant shopping experience. They can shape brand experiences in real-time and in ways that

reflect customer interests and lifestyles. For example, a retailer could use a shopper's in-store location to deliver timely, relevant, and personalized content and offers, such as digital coupons or loyalty rewards.

Optimize Store Operations

Data harvested from IoT sensors and devices will enable retailers to not only better manage store assets, employee labour, and energy usage, but also improve in-store marketing efforts. This operational data will provide real-time insights to store management and employees. For example, smart building technology, including IoT-connected thermostats, lighting, refrigerators, and freezers can manage energy usage. At the same time, in-store IoT-enabled smart cameras, beacons, and sensors can be combined with real-time location data from apps on smartphones to show customer traffic patterns and buying behaviour. Employees can quickly react to bottlenecks, reducing customer wait times.

Improved Inventory and Supply Chain Management

Retailers not only want to know what products are selling but also why. To help answer that question, they need to know who is buying those products, where (in the store) those products perform the best, and any other information that can better predict future sales. IoT solutions can help retailers monitor and track inventory in new ways. For example, IoT-enabled systems can trigger real-time inventory actions based on data from high-resolution cameras and sensors on packages, shelves, and other assets.

IoT data also can be analysed to help understand what's underperforming and overstocked, what's running out of stock and the impact of time of day, weather and other environmental conditions, online trending, and countless other potential variables.

Capture New Revenue Opportunities

Leading-edge retailers will learn how to take advantage of the IoT to seek out new methods of acquiring customers and increasing revenues. The customers' waiting time will be utilized by sending text alerts and notifications and increasing shopping time. The next revolution will be connecting homes with retail stores. Items will be replenished faster and conveniently. For instance, the kitchen and refrigerators can automatically order groceries, and the button on the washing machine will order detergent.

Customers are more empowered than ever before. Creating real, relevant connections with them has become extremely challenging. Retailers that lead in the adoption of IoT systems and solutions will gain an important advantage in a hypercompetitive environment.

Retailers that want to be innovative and stay current with the latest technologies need to embrace the IoT and embed it into their operations, not only to impact front- and back-office process efficiencies but also to earn the loyalty of next-generation consumers.

2.3.13 Smart Supply Chain

An IoT-enabled supply chain system will be an intelligent interconnected network through sensors and other intelligent devices that will connect suppliers, manufacturers, service providers, distributors who are physically located in different regions. The information collected,

processed, and analysed will improve visibility on objects' status and inject flexibility to change status in real-time.

Systems and smart objects with embedded intelligence will be able to make certain decisions and adjust automatically to complex situations. IoT's ability to monitor continuously, sense constraints, and respond almost instantaneously under the guidance of an autonomous system or an intelligent network, will create significant opportunities for cross-enterprise process optimization and innovation. In turn, this would reduce cost and time to market.

The IoT-enabled supply chain would also impact the supply chain organization structure. Skill sets of supply chain professionals will need a transformation from handling the conventional model of the supply chain to a data-driven model in a collaborative cross-enterprise environment.

Deployment of IoT in the supply chain can improve customer satisfaction by reducing time to market, sharing goods status in real-time and reducing risk. The supply chain organizations will improve on profitability, asset utilization, waste reduction, sustainability, equipment/product uptime, security, agility, and risk mitigation. The traditional supply chains havedifferent challenges such as uncertainty of cost, complexity, and vulnerable problems. To overcome these challenges the supply chains must be matter. For establishing a largescale of smart infrastructure for supply chain management to merge data, information, products, physical objects and all processes of supply chain, IoT is the prospective solution (Basset, 2018)

2.3.14 Smart Farming

The Internet of Things will transform the agriculture industry and enable farmers to overcome challenges like increasing water shortages, limited availability of lands, difficulty to manage costs while meeting the increasing consumption needs of a global population that is expected to grow by 70% by 2050 as per Food and Agriculture Organization of the United Nations.

New innovative IoT applications are addressing these issues and increasing the quality, quantity, sustainability, and cost-effectiveness of agricultural production. IoT helps in better crop management, better resource management, cost efficient agriculture, improved quality and quantity, crop monitoring and field monitoring etc by using air temperature sensor, soil pH sensor, soil moisture sensor, humidity sensor, water volume sensor etc (Dagar, 2018).Today's large and local farms can, for example, leverage IoT to remotely monitor sensors that can detect soil moisture, crop growth, and livestock feed levels, remotely manage and control their smart connected harvesters and irrigation equipment, and utilize artificial intelligence-based analytics to quickly analyse operational data combined with 3rd party information, such as weather services, to provide new insights and improve decision making.

IoT sensors capable of providing farmers with information about crop yields, rainfall, pest infestation, and soil nutrition are invaluable to production and offer precise data which can be used to improve farming techniques over time to maximize yields and minimize waste.

Another direction in which smart farming is headed involves intensively controlled indoor growing methods- small indoor farming environments that monitor/administrate specific growing environments and an open-source platform to collect and share data. The collected data is termed a "climate recipe" which can be downloaded to other personal food computers and used to reproduce

climate variables such as carbon dioxide, air temperature, humidity, dissolved oxygen, potential hydrogen, electrical conductivity, and root-zone temperature. This allows users very precise control to document, share, or recreate a specific environment for growing and removes the element of poor weather conditions and human error. It could also potentially allow farmers to induce drought or other abnormal conditions producing desirable traits in specific crops that wouldn't typically occur in nature.

With a future of efficient, data-driven, highly precise farming methods, it is safe to call this type of farming smart. We can expect IoT will forever change the way we grow food.

2.4 Architecture of IoT

There are different standards for IoT architecture. Some researchers mentioned three-layered architecture with Application, Network, and Perception layers, and some of them referenced four-layered architecture with the additional support layer. Some researchers explained five-layered architecture with the Business layer. This study is throwing light on five-layered architecture which is depicted in the figure and explained as follows:

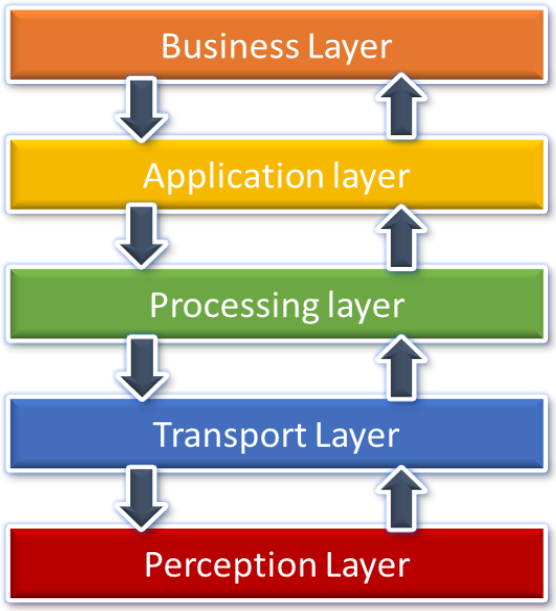

Figure 2-2:Five layered IoT architecture

2.4.1 Perception Layer

The bottom layer of IoT architecture is the perception layer. It is also known as the object layer. The main responsibility of the perception layer is to collect data from heterogeneous devices and then process and digitize the data. It also transfers the processed data into upper layers of IIoT architecture (Bilal, 2019). There are different types of sensors attached to objects to collect information. Therefore, many security threats in this layer is related to sensors. The common security threat at this layer is eavesdropping. This attack is also known as sniffing and snooping. The attacker keeps a small software on the network to passively listens to network communications to gain access to private information, such as node identification numbers, routing updates, or application-sensitive data. The private information is used by attackers to compromise nodes in the network, disrupt routing, or degrade application performance. Cryptography is the standard defence

against eavesdropping attacks. However, due to the limited computing power of sensors, it is difficult to achieve efficient cryptography.

2.4.2 Transport Layer

The transport layer is responsible for end-to-end communication over a network. It also adds features like reliability, congestion detection and avoidance, connection-oriented delivery, same order delivery, data integrity, flow control, traffic control, multiplexing, and byte orientation for seamless delivery of data packets.

In IIoT, this layer takes the responsibility for connecting the smart things, network devices, and networks to each other which makes it highly sensitive to security issues regarding integrity and authentication of information that is being transported in the network. Denial of Service (DoS), Man-in-The-Middle (MiTM), Storage Attack, Exploit Attack are some of the common security threats at the transport layer.

2.4.3 Processing Layer

It's a middleware layer with the responsibility to collect the information from the transport layer. It performs processing onto the collected information and eliminates extra information to retain meaningful information. Several attacks can affect the processing layer and disturb the performance of IIoT. Viruses, Spyware, Adware, Trojans horses, Worms are the common threats at the processing layer.

2.4.4 Application layer

The main objective of IIoT is to ensure effective communication between objects and build a sustained bond among them using different types of applications. The application layer is responsible for determining a set of protocols and providing stable communication among different applications. Some of the commonly used protocols at the application layer are XMPP, MQTT, CoAP, Restful, DSS, AMqP, and Websocket.

The application layer is also vulnerable to security threats and some of the common threats are distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks.

2.4.5 Business Layer

The objective of this layer is to control the whole system, information flow, maintain security, and most important is maintain business logic. It also can determine how information can be created, stored and changed (Rehman, 2018).

The most common security problems with the Business layer are business logic attack which is a cause of flaw in programming. A zero-Day Attack is another threat that refers to a security hole or a problem in an application. Zero-day is a flaw in the software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. (Rouse, 2019).

2.5 Security Concerns of the IoT

Information security refers to the processes and methodologies which are designed and implemented to protect the print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption (Fruhlinger, 2020). Information security can be summed up as the preservation of the confidentiality, integrity, and availability of information and information resources (Watkins, 2012). A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. A security event refers to an occurrence during which company data or its network may have been exposed. And an event that results in a data or network breach is called a security incident (Rosencrance, 2019).

To understand security threats and their treatment, it is important to understand vulnerability. In cybersecurity, a vulnerability is a weakness that can be exploited by a cyber-attack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data (Tunggal, 2016).

There are several security solutions available to deal with cyber-attacks however, no enterprise can overcome all security threats. The attackers are always a step ahead to find the weaknesses in the systems. Hence, it is important to understand the vulnerabilities and mitigate those. Despite the best efforts of cyber and information security professionals, it seems like cybercriminals are always one step ahead of us. They can fly under the radar for long periods, make it difficult to detect and prevent them from penetrating our systems. As a result, cybersecurity is an ever-evolving undertaking, and businesses must reassess their security tools regularly (Secure360, 2016).

There are numerous ways invented by attackers to find vulnerability and attack however topmost threats are as follows:

2.5.1 Insider Attack

When individuals close to an organization and who have authorized access to legitimate information, intentionally or unintentionally misuse the access to negatively affect the organization. Some of the common methods to reduce insider attacks are provide limited access, frequent password change, credentials created with expiry dates for contracts, regular training to employees to follow security protocols and multifactor authentication, etc.

2.5.2 Virus and Worms

The virus and worms are a type of malicious code or program written to alter the way a computer operates. It is designed to spread from one system to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros to execute its code. The virus and worms have the potential to cause unexpected or damaging effects by corrupting or destroying software and data. To reduce the risk of virus and worm attacks, organizations should install antivirus software on computers and network devices and update the latest patches regularly. The modern solution for prevention from viruses and worms is endpoint detection and response (EDR) to take preventive actions to keep endpoints safe from these attacks.

2.5.3 Botnets

A botnet is a network of computers and devices infected by malware that are in control of a single party known as Bot-Header. Cybercriminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft, and distributed denial of service (DDoS) attacks. Some of the measures which can prevent botnet attacks or reduce its impact are, internal and external penetration test to find misconfigurations and vulnerabilities, block malicious activities at the firewall, isolate workloads from one another and secure them individually using micro-segmentation (Bednarz, 2018).

2.5.4 Drive-by download attacks

The unintentional download of a virus or malware onto the computer or mobile device by using a browser, application, or operating system that is out of date and has a security flaw. The drive-by download attacks can be prevented by regularly updating and patching systems with the latest versions of software, applications, browsers, and operating systems. Use web filtering to prevent users' access to blacklisted websites. Web-filtering products can potentially prevent people from going to sites compromised by drive-by downloads internet sites (Levinson, 2012). User awareness to stay away from insecure websites is very important.

2.5.5 Phishing attack

The fraudulent attempt through electronic communication such as email to attain sensitive information or data for instance usernames, passwords, debit cards, and credit card details, by

concealing oneself as a trustworthy entity is known as a phishing attack. Email phishing is the most common phishing attack. Most phishing attacks are sent by email (Irwin, 2020). Spread phishing, Whaling, Smishing & Vishing, and Angler phishing are other known phishing attacks. The recommended techniques to safeguard from phishing attacks are, be aware of new phishing attacks to not fall prey to it, develop a habit to think before you click on a link, install an anti-phishing toolbar, be wary of pop-ups you receive, use anti-virus software and keep it up to date, keep internet browser up to date and inform your organization's cybersecurity team if you face phishing attack.

2.5.6 DDoS Attack

In a distributed denial-of-service (DDoS) attack, multiple compromised systems attack another system, for instance, a server, website, or a network device by sending a flood of traffic to make it inoperable and deny service to the legitimate system or user. DDoS attacks are growing very fast and there is no single tool available to prevent them. Global information and technology provider Neustar reported that it found a 168% increase in DDoS attacks in Q4 2019 from Q4 2018. Overall, there was a 180% increase in DDoS attacks in 2019 compared with 2018 (DSM, 2020). Following are the recommendations from security experts for prevention from the attack or to mild its impact, a response plan for DDoS attack, a multi-layer solution to protect, VPNs, firewalls, DNS, emails, endpoints, servers, and other network devices.

2.5.7 Ransomware

Ransomware is a form of malware that blackmails its victim. The name "ransomware" comes from the ransom note asking its victim to pay some money (ransom) in return for gaining back

access to their data or device, or for the attacker not to divulge the victim's embarrassing or compromising information (Hull, 2019). Globally, a total of 199.7 million ransomware attacks have been reported in the third quarter of 2020 (Das, 2020)**.**According to the Cisco 2017 Annual Cybersecurity Report, ransomware is growing at a yearly rate of 350%. As its ransomware is going very fast, all organizations must deal with it. Some of the best practices advised by experts are, keep a good copy of the backup to restore your files, Do not provide personal information when answering an email, unsolicited phone call, text message, deploy content scanning and filtering on mail servers and gateways, Make sure you use a trustworthy VPN when accessing public Wi-Fi (Norton, 2018).

2.5.8 Exploit Kit

An exploit kit or exploit pack is a type of toolkit cyber criminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities. Exploit kits are packaged with exploits that can target commonly installed software such as Adobe Flash, Java, Microsoft Silverlight (Trend Micro, 2020). The protection measures from exploit kit attacks are the same used for other attacks too, for instance, keep browsers and plug-ins updated, use vulnerability assessment tools and take proactive action for vulnerabilities, deploy modernize endpoint protection tools like endpoint detection and response for proactive action against viruses and malware, etc.

2.5.9 Advanced Persistent Threat attacks

An advanced persistent threat (APT) is a cyberattack in which an intruder infiltrates a network through a compromised or week perimeter device, applications and remains unnoticed until gets

confidential information and data. The objective of APT attacks is not to damage the system or network. Attackers intend to monitor network activities and steal security information like encryption models to breach security and steal salient information of an organization. Once a threat actor determines that they have established reliable network access, they gather target data, such as account names and passwords. Even though passwords are often encrypted, encryption can be cracked. Once that happens, the threat actor can identify and access data (Fireeye, 2020). To defence against APT attacks are, encryption-based VPN tunnel for user access to the network, modernized firewalls to protect the network from outside traffic, inspect HTTP traffic by deploying web application firewall, email protection at email gateways and measure against phishing emails, strong protection for endpoints using latest anti-virus and endpoint detection and response solutions and so on.

2.5.10 Malvertising

The technique of this attack is like a phishing attack. In malvertising, cybercriminals inject malicious code through legitimate online advertisements. On accessing these advertisements, the malicious code redirects users to malicious websites or installs malware on their computers or mobile devices. Cybercriminals use malvertising to deploy a variety of moneymaking malware, including crypto mining scripts, ransomware, and banking Trojans (Rosencrance, 2019). Malvertising is a major threat for the online advertising industry and digital marketing to lose revenue and brand reputation. As per clean.io who provides cybersecurity services, in 2019, ads that were served via programmatic exchanges were hit by malvertising that cost publishers $325M. In 2018, ad fraud caused digital advertisers to lose $19B, or about 9% of their total spend for digital advertising. Publishers lose about $1.3B a year to malvertising. By 2022, digital ad fraud could cost

$44B in lost revenue (Clean.IO, 2020). Web hosting organizations and end-users need to take precautions to prevent malvertising attacks. There are technical security measures for instance updated anti-virus and patch updates, web application firewall, intruder detection and prevention systems, modernized firewall, etc are vital security measures for the end-user as well as web-hosting organization. These solutions accompanied by governance from web hosting organizations are proved effective in the prevention of malvertising attacks for example, through verification of advertising sites and paperwork before publishing ads.

2.6 The sequence of Security Threats on IoT

The IoT is a web of multiple devices, sensors, servers, computers, etc. IIoT stands for the Industrial Internet of Things or Industrial IoT that initially mainly referred to an industrial framework whereby a large number of devices or machines are connected and synchronized through the use of software tools and third platform technologies in a machine-to-machine and Internet of Things context, later an Industry 4.0 or Industrial Internet context (i-Scoop, 2015). It makes IIoT more vulnerable to security attacks as attackers can find many loopholes to get access to hardware and software as an entry point. IoT devices are vulnerable largely because these devices lack the necessary built-in security to counter threats. Aside from the technical aspects, users also contribute to the devices' vulnerability to threats (Trend Micro, 2020). IoT devices run on low power and less computing resource capability. Due to this, they cannot afford to have complex security protocols. Hence, it becomes an easy target for intruders (Smith, 2020). To keep low cost of the solution, the IIoT solution providers keep focusing on computation and the availability of devices. The focus on security remains low. There is a set of sequences followed by attackers to have control of the IIoT ecosystem which is explained as follows:

2.6.1 Exploitation

When an attacker can find a vulnerable device, he can install the software to monitor the traffic and gain access to other devices. When an attacker can compromise an IoT device, they may install their software and use the device in nefarious ways (SCHNEIER, 2014). The access of vulnerable devices is the first step for attackers in further exploitation of the system.

2.6.2 Persistence

Once the attacker has control of the hardware and software of the IIoT ecosystem, he can stay there unnoticed for some time and observe communication among devices and take control of more devices and software gradually. APT are sophisticated, professional, state-supported, and systematic cyber-attack programs that continue for an extended period and in which a group of skilled hackers coordinates to design the attack with a particular motive, targeting specific information in high-profile companies and governments (Khan, 2019). The attackers pursue privilege escalation and perimeter expansion using malware through email or USB drives and then remain concealed inside the critical systems to collect intellectual property and other assets information for further disruption or observation.

2.6.3 Steal Data

Once hackers can establish control, it is time to start the activity he has come for, organizations' confidential data stealing. Confidential data is personally identifiable information (PII) that you

don't want anyone to obtain without your permission. This may include Social Security number, Phone numbers of friends/family/colleagues/students, Driver's license numbers, Bank account numbers, Tax information, Passwords or passphrases, Home address or phone numbers, Employee ID number, Digital images, Any personal electronic documents containing personal text. If any PII you are storing is stolen, the perpetrator could alter the information and use it to commit identity theft (IOWA, n.d.). Most often, attackers remove the data or confiscate data for a certain period from the network and storage devices.

2.6.4 Data Tampering

Removing or confiscating data is not always the motive of attackers, sometimes they intrude with intention of tempering data to harm organizations' brand image**.** Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorized channels. Data exists in two states: in transit or at rest. In both instances, data could be intercepted and tampered with (Griffin, 2020). Data tempering has a devastating impact and it has been taken seriously by cybersecurity organizations of counties. Several laws are amended to protect data from tampering. As per the 85th Texas Legislature created a new law in 2017, a person commits an offense if the person intentionally alters data as it transmits between two computers in a computer network or computer system through deception and without a legitimate business purpose (Saputo, n.d.).

2.6.5 Access traffic between two devices

Data stealing and data tempering is not the only motive of attackers, they can access traffic and move to it to illegitimate sites. The attackers intercepted important data using different techniques to interject themselves into the communication process which is also known as Man in the Middle attack (MitM). Though it can be protected against with encryption, successful attackers will either reroute traffic to phishing sites designed to look legitimate or simply pass on traffic to its intended destination once harvested or recorded, meaning detection of such attacks is incredibly difficult (Swinhoe, 2019).

2.6.6 Impact on important services through illegitimate traffic

The other way to attack is by sending a flood of traffic from illegitimate sites to applications, TCP port, and bandwidth to reduce the performance or chock it all together. Such type of attack is called Denial of Service attacks (DDoS). A Distributed Denial of Service (DDoS) attack is an attempt to crash a web server or online system by overwhelming it with data. DDoS attacks can be simple mischief, revenge, or hacktivism, and can range from a minor annoyance to long-term downtime resulting in loss of business (Peter, 2020).

2.7 Specific Security Challenges for IIoT

2.7.1 Insufficient Testing

IoT is a network of small and big devices, machines, sensors that are manufactured by small and large organizations. To build a cost-effective solution, the IoT solution providers opt for high,

medium, and low-cost devices. The manufacturing companies that build low-cost devices did not pay enough attention to security design and testing to find manufacturing gaps. These gaps become a target for attackers to intrude once devices are connected to IoT systems. One of the main problems with tech companies building these devices is that they are too careless when it comes to the handling of device-related security risks (Harper, 2016).

2.7.2 Multivendor Interoperability

As IoT is build using many wired and wireless devices which are manufactured by different manufacturers. These devices need strong interoperability to give a secure solution. The week connectivity of two devices can be an attraction for hackers as a point of entry. Besides the capability of some devices to be able to mechanically bond with other devices, it means that the users and the developers of IoT all have an obligation of ensuring that they are not exposing the other users as well as the Internet itself to potential harm. A shared approach required in developing an effective and appropriate solution to the challenges is currently witnessed in the IoT (Alaba et al., 2017).

2.7.3 Patching and Software updates

Updating operating system and software patches are key to keep the IoT ecosystem secure. This is a major challenge due to many devices are connected and getting their updates at the same time which gives opportunity to hackers to use vulnerability and attack. Usually, IoT manufacturers update security patches quarterly. The OS versions and security patches are also upgraded similarly.

Therefore, hackers get sufficient time to crack the security protocols and steal sensitive data (Delipi, 2016).

2.7.4 Device Monitoring

Monitoring so many devices of different makes and models is another security challenge for IIoT. Firstly, finding a solution that can cater to monitoring requirements for IIoT devices is a challenging task. Over and above, monitoring data analysis and assign an action for the right technical person to solve it, is another challenge. IoT devices that do more than simply spit out data are significantly more critical to the operation of a business, which means that their health should be monitored very closely. At a high level, the act of monitoring these devices is the same as for others, but because metrics might not be their core functionality, the actual method of monitoring will likely be more involved (Flower, 2016).

2.8 Security Framework

IoT is going to be an established part of the industry by extending communication and networking anytime, anywhere. A properly formulated, implemented, and enforced security policy is the underline requirement for the IoT ecosystem. Having a foolproof Security framework is a must to get maximum advantages from IoT. Increasingly, researchers have developed many frameworks to build a secured IoT ecosystem. Embedded Security for IoT will be crucial and important with strong security mechanisms which will prevent damages and economical losses offering new business opportunities. However, sound security solutions are not attained easily (Babar, 2011). Following are the key features to be considered to develop a

security framework. Lightweight cryptography, standardized security protocol, physical security, secure operating system, future application area, secure storage (Babar, 2011). The researchers have also suggested secure authentication mechanisms using certificate-based credentials are the key to securing the IoT (Ramos et al., 2015). Finally, (Tan et al., 2007) made an argument for the combination of all security models, through a semantic approach, taking advantage of the decision-making ability of autonomous nodes, based on domain knowledge. The following are the proposed area to be kept secure to have a secured IoT environment.

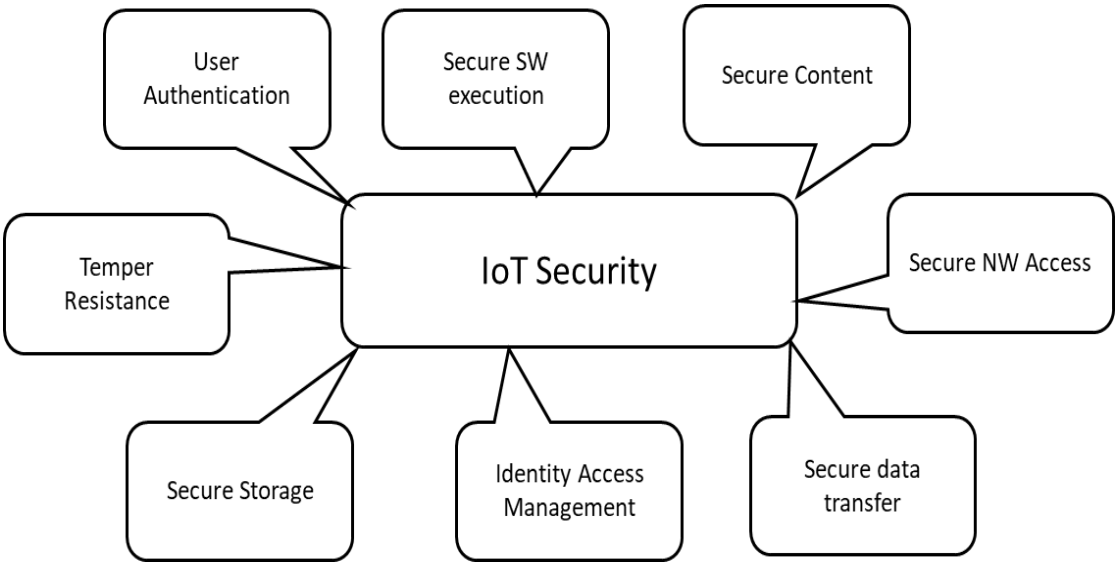

Figure 2-3: IoT Security

The security for IoT is imperative however, it's not possible to get one solution that can protect end to end IoT ecosystem. The security threats have to be carefully studied at each layer and suitable solutions to be implemented. The above figure shows different security threats for each layer and mitigations for those threats.

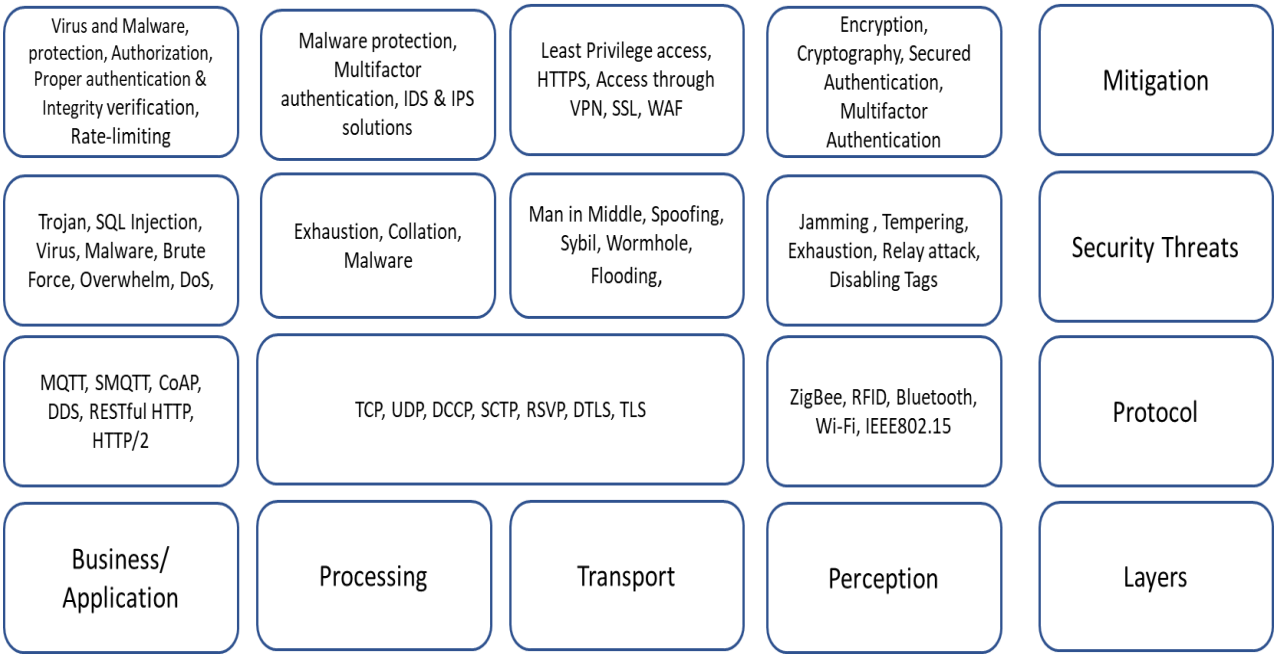

Figure 2-4:Proposed security model

The SOAR is the latest solution available that can support organizations to deal with increasing threats. SOAR stands for Security Orchestration, Automation, and Response. The term is used to describe three software capabilities – threat and vulnerability management, security incident response, and security operations automation. SOAR allows companies to collect threat-related data from a range of sources and automate responses to low-level threats.

2.9 Ethical and Legal Issues of the IoT

IoT works with three types of interaction, people to people, people to things, and things/machines to things/machines. Therefore, since IoT does not concern objects only but also interrelations between objects and humans, there is a strong need to consider the philosophical, ethical, and legal issues of IoT cohabitation with humans (Tzafestas, 2018). IoT technologies can

solve many industrial problems but they create serious ethical concerns and legal challenges related to, protection of privacy, data security, data usability, data user experience, trust, and safety, etc.

2.9.1 Privacy

In the IoT landscape, most of the time privacy is compromised which is a major issue. Data privacy and information privacy are synonyms. It means data protection and proper handling of sensitive data including personal data, financial data, intellectual property data, and other confidential data as per regulatory requirements. Data protection spans three broad categories, namely, traditional data protection (such as backup and restore copies), data security, and data privacy as depicted in figure below. Ensuring the privacy of sensitive and personal data can be considered an outcome of best practices in data protection and security with the overall goal of achieving the continual availability and immutability of critical business data. There are many times when data privacy and security are misunderstood. It is mistakenly believed that keeping personal and sensitive data secure from hackers means that they are automatically compliant with data privacy regulations. This is not the case. Data security protects data from compromise by external attackers and malicious insiders whereas data privacy governs how the data is collected, shared, and used.

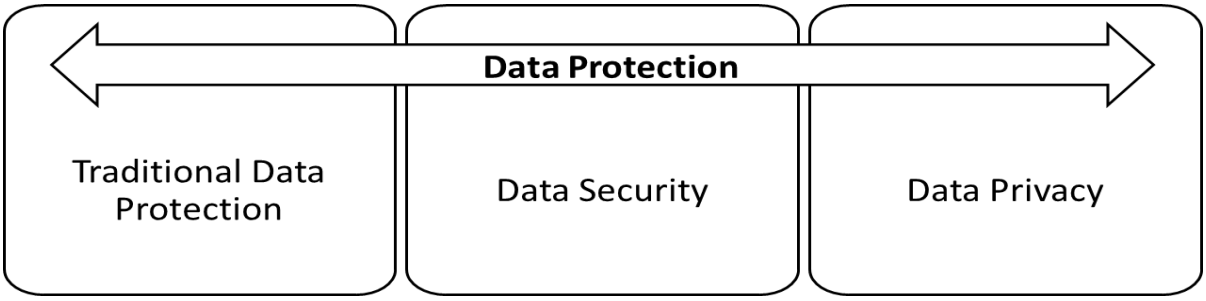

Figure 2-5: Data protection categories

As IoT comprises multiple devices which consistently share data, so it's very easy for hackers to finds any week point which is left unattended from security protection solutions. It is a proven challenge in privacy protection in the IoT landscape. When it comes to privacy and IoT, there are two types of data. Location privacy involves protecting the information of personal location and data privacy involves the protection of sensitive personal information (Sen, 2011). 60% of IoT devices falling short on privacy and data protection (Wray, 2016).There have been several cases of concern for personal information tracked on RFID tags, including German Passports and FIFA Football World Cup tickets (Friedewalda, 2011).

2.9.2 Safety

Safety means keeping yourself and others safe from any harm, injury, and loss. Safety is a state in which hazards and conditions leading to physical, psychological, or material harm are controlled to preserve the health and well-being of individuals and the community. It is an essential resource for everyday life, needed by individuals and communities to realize their aspirations (Quebec, 2020). The safety concerns due to breaches of security are another area of

concern in the IIoT ecosystem. The control taken by hackers on devices, machines, and sensors can have devastating results which could end up serious accidents.

The implementation of IoT in the medical industry can be impacted significantly because of the security breach. The recent Vectra 2019 Spotlight Report on Healthcare indicates that the proliferation of healthcare internet-of-things (IoT) devices, along with a lack of network segmentation, insufficient access controls, and reliance on legacy systems, has created an increasing attack surface that can be exploited by cybercriminals (Arampatzis, 2019). When it comes to healthcare the IoT can refer to a wide variety of crucial and sensitive devices such as heart monitoring implants, infusion pumps, pacemakers, insulin pumps, that provide a pre-programmed level of fluids into patients in the hospital and many more devices like continuous glucose monitoring, hearing aids, heart rate patches and wireless scales for monitoring congestive heart failure, sensors in shoes to detect falls and gait changes, baby monitors with temperature, heart rate, and other sensors, patient identification and tracking, diabetes care devices and mobile ECGs. Some of these devices like the pacemaker sends information through a wireless connection, while others can send and receive information. The malfunctioning of such medical equipment due to vulnerability can result in taking the life of patients. The main priority for healthcare organizations is to protect patients and their personal information, which means more thorough work with hardware and software developers on security and privacy issues with IoT in healthcare (Mykola, 2020). In the last few years, cyberattacks on healthcare institutions have caused several problems. They disrupted many of their vital services, caused financial losses, and lowered patient confidence in the entire healthcare system. They've also posed risks to the very safety of patients' health (Atoui, 2020).

The pharmaceutical manufacturing industry is another area that is impacted by security attacks and faced huge losses. The minor changes in the quantities of chemicals and salts of medicine can cause major health issues of patients and impact the reputation of a manufacturing organization which can be a key motive of the intruder. When it comes to medicines and healthcare utilities, it is as important as anything else that there should not be any alteration in the specifications of the product while in transition from manufacturing units to the consumers. The dependency on monitoring through IoT has increased in the coming days during the transition and any alternation in monitoring data can change the analytics which will be unnoticed by the manufacturer and end up impacting the health of the consumer. While almost every sector is getting more and more data-intensive and deploying resources to maximize the utilization of the available data for analysing the trends and accordingly developing the business models. For the pharmaceutical industry as well, this is a great opportunity. But simultaneously it is an equally big challenge. Two major challenges are, building datacentres capable of handling the data and ensuring cybersecurity from the attackers who are chasing all kinds of the data breach; from intellectual property, commercially critical data to patient's private health data from the research labs (Marathe, 2018).

The food industry is another area where IoT is used significantly and impacted by vulnerabilities. The attackers are attracted towards the food in industry as the alteration in the production can have an impact on consumer health and can damage the reputation of organizations.

The safety and security of factory workers who are dealing with heavy machines is also an area of concern. The control made by hackers on the machines can cause accidents which can be harmful to factory workers.

2.10 Ethical Issues in IoT Due to Security Concerns

Ethics is a branch of philosophy that defines human conduct and behaviour in society. Ethics considers what is morally right or wrong, just or unjust, while rationally justifying our moral judgments. Ethics in the IoT context deal with defining the regulation to safeguard human, personal, and public property and reputation which can be compromised due to IoT security concerns. The IoT is changing everything about the manufacturing industry, the production of goods, the supply chain, workers' interaction with machines, etc. Consequently, there is a need to develop an ethical framework that helps ensure the protection of manufacturing organizations' interests, reputation, and most important employees' safety and security. Due to the complexity, heterogeneity, and large scale of the IoT system, new ideas and thoughts should be presented to define the appropriate regulation and policies for this complex environment (Atlam, 2019). Ethical issues in the IoT are mainly caused by the expansion of IoT technologies (Alenezi, 2017). In addition, as the community continues to explore the risks and opportunities associated with IoT-driven systems, attention to transparency and the ethics of these systems' use and behaviour needs to be a core part of the discussion. In addition, there is the intensive requirement to build a framework to explain the guidelines of ethical practice in manufacturing industries to remove ambiguities. The mechanisms that enforce ethical IoT frameworks need to be relevant to an ecosystem that includes humans, autonomous and self-determining systems, devices, and virtual and physical environments (Baldini, 2018).

2.11 Legal Issue in IoT

With an innumerable number of devices connected in the IoT ecosystem communicating to each other via the internet, the potential for a data security breach is high and there is a need to define regulations to protect service provides, users of IoT, and end customs. The Information Act 2000 is in place to protect individual personal information. The Information Technology Act, 2000 ("ITA") and the "Reasonable practices and procedures and sensitive personal data or information Rules, 2011" ("Rules") issued under Section 43A of the ITA (as amended deals with the protection of data in an electronic medium and provides that when a body corporate is negligent in implementing and maintaining 'reasonable security practices and procedures about any 'sensitive personal data or information that it deals, possesses or handles in a computer resource that it owns, operates or controls and such negligence causes wrongful loss or wrongful gain to any person, such entity shall be liable to pay damages by way of compensation to the person so affected (Sarin, 2018). However, this act has many limitations. The cyber laws particularly the laws of data protection and data security in India are in the nascent stage and are still developing, with the only significant legislations being the Information Technology Act, 2000 (ITA) and the reasonable practices and procedures and sensitive personal data or information Rules, 2011 (Sarin, 2018). With the paucity of regulation, the legal issues of an IoT security breach can be addressed only by drafting and executing agreements between all stakeholders to safeguard the interest of IoT service providers, the organizations using IoT service, and the end-user.

2.12 Practical Issues with the IoT

Besides the security, legal and ethical issues there are other concerns in IoT which must be addressed to take its full advantages like standardization and compatibility.

2.12.1 Standardization

In IoT, plenty of connected smart objects produce enormous data. There is a requirement to store, process, and transfer the data which needs standardization for unified operations. Standardization is to achieve universally accepted specifications and protocols for true interoperability between devices and applications to ensure secure and cost-effective solutions. The need for standardization increases when different vendors are involved in providing the solution. As security is very crucial for the IoT world, standardization is important for IoT. It will also help create a level of consistency when dealing with firewalls, backend tasks, and more. Many have suggested that a standard model for the IoT might be able to help resolve some of the issues faced by the industry today. IoT is not only plagued with security, authentication, and access control issues, it doesn't work as well with the fourth industrial revolution, commonly known as Industry 4.0. The absence of effective regulation, standards, and weak governance has led to a continual downward trend in the security of IoT networks and devices, as well as given rise to a broad range of privacy issues (Saleem, 2018).

2.12.2 Compatibility

Interoperability of different devices is another challenge in the IoT world. There are different devices, connectors, sensors manufactured by multiple vendors that are a real challenge in using

those together. To optimize IoT cost, many manufacturers tend to use old machines, and the connectivity of such machines not ready for the IoT ecosystem is another challenge. The New waves of technology often feature a large stable of competitors jockeying for market share, and IoT is certainly no exception. This can be good news since competition creates increased choices for consumers, but it can also create frustrating compatibility issues (D'mello, 2020).

2.13 Governance Challenges of the IoT

From a manufacturing management perspective, the IoT shows some unique Challenges which need to form strong governance to take maximum benefits of IoT. Governance, security, and privacy are probably the most challenging issues in the Internet of Things (Levitt, 2015). These governance covers, holistic program management for IoT implementation, security management, training and awareness management, and monitoring management. Each facet of IoT governance requires an adjustment to align with the reality of the IoT. The concept of Governance has been already applied to the different areas of the Internet for specific matters and there are organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, W3C in place which are responsible for building and controlling governance for their respective areas. Even though these organizations have established governance, however, IoT-focused governance to cater to the needs of industry, service providers, and consumers is not in place. The difficulty is that the high number and heterogeneity of technologies and devices in the IoT require even more specific Governance solutions and approaches that are more complex (Levitt, 2015). IoT governance is one of the key remaining challenges. Achieving the right governance framework is critical to IoT's success across all aspects from architecture, through standards to implementation (Levitt, 2015).

As security and privacy are challenges for IoT landscape, it is important to understand its governance challenges.

2.13.1 Context-based Security and Privacy

Context-aware security requires knowledge of who the user is, what the user is requesting, how the user is connected, when the user is requesting information, and where the user is located. There is a major need to build a security framework to provide a context-based security model for IIoT.

2.13.2 Cyber-Physical Systems and IIoT

The systems in which machine is controlled by algorithms. These machines take information from other intelligent systems and work. However, these machines are not intelligent and not design to be protected from security attacks. The interoperability of intelligent systems with such machines incorporates high risk to human life who are operating these machines at the time of malware attacks. Hence, strong governance to build a security framework to handle interoperability issues is expected.

2.13.3 Identification in a Distributed Environment

Identification is closely tied to IoT governance, security, and privacy. The identification of devices used in the IoT ecosystem is a key component of multiple layers of IoT. Any form of identifications like naming, numbering, and addressing has a set of influencing factors that create. The IoT environment can identify the latest devices connected while there is a legacy environment

that cannot be ignored and must be addressed in some or other way. Many of the existing naming, numbering and addressing schemes have been created to address specific objectives at one point in time and therefore there is no one universal answer to identification that can provide for all of IoT's requirements without limiting IoT's scope or diminishing IoT's applicability (Levitt, 2015). To succeed IoT and spread its usage, it requires an established governance body to maintain and control identification. Until central controlling authority is in place, discussions about identification schemes and governance models are likely to be inconclusive.

2.13.4 Device Authentication

An effective authentication framework for IoT devices provides appropriate protection against cyber threats. Authentication for the IoT devices is different from common authentication methods prevailing. Due to potential resource constraints, it needs lighter-weight authentication. The major challenge which the industry is facing with IoT today is, it is lacking established industry standards for authentication which have forced IoT vendors to develop proprietary authentication methods. Since many IoT devices can be resource-constrained with low computing power and storage capacity, existing authentication methods are not a good candidate due to their significant bandwidth and computational requirements (Singh, 2019). There is a rising need to streamline devices and service authentication for the IoT ecosystem. It is important to analyse and use the factors essential for verifying the identity of 'things to establish the desired level of trust in the device's identity without overburdening the fit-for-purpose computing abilities of the IoT device (Singh, 2019).

2.14 Software Development Challenges of the IoT

IOT software development plays a crucial role in delivering a successful and secure IoT solution to the industry. Many challenges in IoT are different from the common challenges of usual software development.

The IoT solutions require high-quality, scalable, robust, secure, and user-friendly solutions. IoT development teams need to assess all these factors to build standard procedures to take everything into account. Due to the booming demand, the competition among IoT start-ups and development companies is knife-fighting level fierce. This and the lack of generally accepted standards make programmers constantly looking for new practices and updated protocols. Only a scrupulous approach to every IoT software issue will result in efficient development (All, 2019).

Some of the challenges which IoT developers face are as follows:

2.14.1 Selection of Operating System

IoT devices are far less powerful and run on relatively small memory capacity, unlike traditional devices. A small battery that can sustain for a longer period is another challenge. This means the developers must choose the matching operating system. The selected operating system must use minimum resources and able to vacate if not in use. The latest IoT Developer Survey shows that Linux is the top choice for IoT microcontrollers, constrained devices, and gateways (Hall, 2018).

2.14.2 Choose Gateway

IoT ecosystem is made up of multiple devices of different make and model which use different protocols for connectivity like WiFi, Bluetooth, Zigbee, Serial port, etc. Gateways are connected between IoT devices and the cloud. Hence, the IoT ecosystem is dependent on the gateway significantly. Being diverse in connectivity and devices, the design of a gateway to cater to all needs is a challenge. It is very difficult to design an IoT Gateway for an application, keeping the future requirements in mind, because there are too many variables that impact the design. The IoT realm is divided with the countless number of vendors and there are almost no widely agreed standards (Labram, 2016). To make the IoT ecosystem works and give desired results, the application development must cater to the mention challenges of gateway design and make sure the heterogeneous connected devices can communicate with the gateway.

2.14.3 Choose Right Platform

IoT platforms provide a packaged solution to start building IoT systems using built-in tools and capabilities to make it easier for businesses, developers, and users. IoT platform helps facilitate the communication, data flow, device management, and functionality of applications. As requirements for the IoT platform varies as per need, it's a challenge for solution providers to build one solution fit for all. IoT developers should note, however, that platforms perfect for smart factories might not fit connected cars or energy consumption solutions (IoT for All, 2019). Here is the challenge for developers to consider the available solutions in the IoT platform rather than reinventing the wheel and integrate it with in-house solutions. Such integrations play a substantial role as any loosely coupled integration can be rewarding for intruders.

2.14.4 Quality Assurance

Quality assurance is another area of challenge for software for IoT. Since IoT devices are used not only for temperature control in warehouses but also for insulin pumps, testing should be eminently thorough. Any small issue can turn out to be deadly, literally (IoT for All, 2019). The variety of testing is enormous in IoT software quality assurance and rigorous security testing is the top priority. In addition to security testing, usability and compatibility should be assured as well. Make sure to include security testing in the software development process from the very beginning (IoT for All, 2019). The test cases for software quality assurance are enormous and vary due to the diversity of IoT ecosystems. A test case suitable for one IoT environment might not use in another one. Hence, standardization of quality assurance is a major requirement.

2.14.5 Maintenance and Monitoring

As the network of interconnected devices in IIoT is growing, monitoring and maintenance become a greater challenge. Different make and model of the device comes with its requirements for software updates and security patches. Asset-intensive industries face a range of challenges to ensure their mission-critical plans and equipment operate at maximum efficiency and uptime. The smallest disruption to service can lead to costly penalties and churn (Reed, 2020). There is a greater need to build standardization in this area which is dependent on the standardization of devices used for the IIoT environment. In the hybrid environment of IIoT where older machines that are not IIoT enabled synched with the latest IIoT devices, is another hurdle in maintenance. The coupling points of such older machines are the loopholes and attractions for intruders. Building a solution to cater

monitoring and maintenance of such a complex environment is a challenge to give a fool proof IIoT solution.

2.15 UTAUT Model

The unified theory of acceptance and use of technology is also known as UTAUT model of technology acceptance. This model is developed by Vishwanath Venkatesh, Michael G Morris, Girden B. Davis, Fred D. Davis in 2003. As UTAUT model is developed to understand user intentions to use an information system, it is widely accepted by many researchers in the area of the adoption of technology. The UTAUT model uses four key constructs: performance expectancy effort expectancy, facilitating conditions and social influence. Gender, age, experience, and voluntariness of use are moderators to further study the impact of four constructs in adoption of information system. Although many models were developed independently on adoption of technology, the popularity and acceptance of UTAUT is due to its consolidation of the constructs of eight models developed by earlier researchers. These eight models are action developed by Martin Fishbein and Icek Ajzen in 1967, technology acceptance model by Fred Davis in 1989, motivational model introduced by Abraham Maslow in 1940, theory of planned behaviour proposed by Icek Ajzen in 1985, a combined theory of planned behaviour/technology acceptance model developed by Taylor and Todd in 1995, model of personal computer use by Triandis in 1979, diffusion of innovations theory by Everett Rogers in 1962, and social cognitive theory byAlbert Bandura in 1977. Venkatesh with others noticed that information system or information technology researchers were confronted with a choice among a multitude of models and were bound to choose constructs across models or choose a favoured model, thus ignoring the contribution from alternative ones. They felt the need for a synthesis to reach a unified view of users' technology

acceptance. They reviewed and compared the eight dominant models that have been used to explain technology acceptance behaviour and developed a consolidated view known as UTAUT (Al-Qeisi, 2009). Cumulatively, theories offered by different researchers explains IS/IT acceptance and usage based on different factors such as technology attributes and contextual factors. Based on a comprehensive review and synthesis of several theoretical models, Venkatesh and others proposed the Unified Theory of Acceptance and Use of Technology (UTAUT), which has since been used extensively by researchers in their quest to explain IS/IT acceptance and use (Dwivedi, 2017).The researchers found that UTAUT has the upper explanatory power compared to other relevant models and theories in IS/IT acceptance context. The UTAUT is the most popular model in the field of technology acceptance and focuses on the technology factors for the successful implementation of information systems (Almaiah, 2019).

The rational for using UTAUT in place of UTAUT 2 model is, the UTAUT has been used to describe users' technology adoption behaviour in organizational context. Instead, the UTAUT2 model was extended from the UTAUT and was focused on individual perspectives in technology adoptions. The additional constructs and moderators used in UTAUT2 are perceived to be useful for study of consumer technologies like mobile phones and laptops etc. As this study is to understand organisations constraints to adopt IoT, the UTAUT model will be suitable for this research.

The constructs in the UTAUT model were defined and related to similar variables in the eight models as follows:

2.15.1 Performance Expectancy (PE)

It explains the degree to which a person believes that using a particular system will help to improve performance. The constructs in the other models that pertain to performance expectancy are: perceived usefulness (TAM, and combined TAM-TPB), extrinsic motivation (MM), job-fit (MPCU), relative advantage (DOI), and outcome expectancy (SCT) (Al-Qeisi, 2009).

Several studies made on this construct give two views. The first view reveals that Performance Expectancy has influence on adoption of new technologies (Sujin Oh, 2009). The other view contradicts the first view (Jennie Pena, 2017).

2.15.2 Effort Expectancy (EE)

It describes the degree of ease of use of a system. The same construct in the other models is used as: perceived ease of use (TAM), and complexity (DOI and MPCU).

The literature review gives two views on this construct too. Several researchers considered it an important construct. However, a contradicting view was also given in many literatures. As it is treated as ease of use of technology, it is an important factor (Sujin Oh, 2009).The contradicting studies find it not an important factor to influence technology adoption (Wonjun Lee, 2018).

2.15.3 Social Influence (SI)

The social influence is the degree to which a person observes the importance of others believe that he/she should use a system. This construct is not included in this study. As explained by Venkatesh et al. (2003), SI significantly influences perceived usefulness via both internalizations,

in which people incorporate social influences into their own usefulness perceptions and identification, in which people use a system to gain status and influence within the work group and thereby improve their job performance, particularly in the early stages of experience (Keong, et al., 2012). This construct is found to be more useful for the users who are very young and lesser experience. Also, this construct impacts consumer-based technologies like mobile phones, tablets and laptops etc. As this study will be conducted on senior staff and owners of the organisations, the SI will not be useful to study.

2.15.4 Facilitating Conditions (FC)

It describes the degree to which a person believes that necessary technical infrastructure is available to support use of the system. This definition captures three different constructs in existing models: perceived behavioural control (TPB/DTPB and combined TAM-TPB), facilitating conditions (MPCU), and compatibility (DOI) (Al-Qeisi, 2009).

Unlike Performance Expectancy and Effort Expectancy, researchers have given one views for this construct in supports of Facilitating conditions influence on consumer intention to adopt technologies. Several studies considered this construct as an important factor in adoption of technologies (June Lu C.-S. Y., 2016).

2.16 List of Most Relevant Literature Reviewed

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	FisnikDelipi 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	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

Table 2-1: Literatures Reviewed

2.17 Research Gap

Based on literature study, following gaps are identified:

- Several studies are made on the adoption of technology but there is no specific research on the IoT adoption for manufacturing organizations in India.
- Various technology adoption models are available and used by several researchers whereas no one has considered security awareness as a factor that can impact the adoption of IoT in manufacturing organisation. As cyber security incidents are increasing, a unified view with security awareness is the need of this age.
- Size of the organisation has a significant role in adoption of technology, and it is important to understand how large, medium, and small size organisations are impacting other factors that are influencing adoption of IoT. There is a need to provide a consolidated view to understand the factors with moderating impact of the organisation size that are hindering adoption of IoT.

2.18 Summary

A literature review is provided on IoT in this chapter. The explanation of IIoT and IoT, its usage in different areas like smart city, smart grid, smart agriculture, etc. The five-layered architecture of IoT is explained in detail along with security threats at each layer and available solutions to mitigate those threats. Thereafter, different security attacks were explained in detail and possible solutions to avoid those threats. The damage to the IoT environment due to these threats is also explained. The attack on data which is the end motive of the security attacker is sequential which was discussed. The multiple security challenges for the IoT ecosystem like multivendor

solutions, lack of testing, compatibility, and monitoring issues. These challenges are showstoppers for a secure IoT solution were discussed. There cannot be one security model which can fit in different IoT ecosystem. However, a security model which can be useful for many IoT ecosystems is proposed post different literature review on the security of IoT. The ethical and legal challenges for IoT environments are also discussed. Standardization, compatibility, and strong governance are key concerns for IoT and cannot be overlooked. Other practical challenges of IoT in software development are also discussed. Quality assurance difficulties in the IoT landscape, maintenance, and monitoring challenges for IoT devices are also explored. Thereafter, the UTAUT model developed by Venkatesh is discussed and its four constructs were explained. Three out of four constructs described in this model will be used in this study. At last, list of important literatures was shared along with gist and their relationship with research. These literatures are part bases of designing this study.

CHAPTER 3:
RESEARCH METHODOLOGY

CHAPTER 3: RESEARCH METHODOLOGY

The chapter starts with defining stages of research process followed by method selected for the study. The purpose of the study along with gaps identified in other studies will be explored. Thereafter, the research question and associated hypothesis will be explained followed by the method selected to analyse the data. The research design will be explained in detail. The target population survey and sample size will also be explained.

3.1 Stages of Research Process

The figure below explains different stages of research that start from identifying the problem through literature review, formation of hypothesis post defining research questions, define research methodology followed by identifying population and size of pollution from whom data will be collected through the survey. The pilot study is an important phase in the study which will provide information to finetune the main study. Final milestone is data collection and analysis.

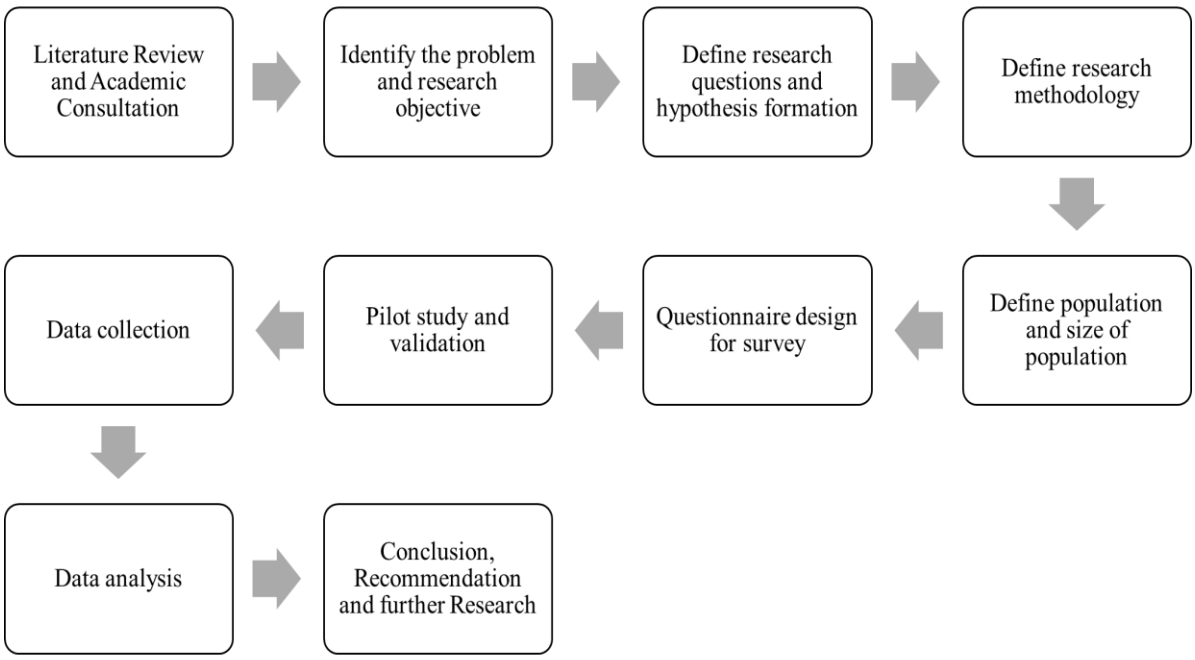

Figure 3-1: Stages of research process

3.2 Problem Identification

The topic of research is the factor affecting the adoption of the Internet of Things in the Indian industry. A study in the manufacturing industry in and around Mumbai. It is observed that awareness of security threats is a major concern in the adoption of IoT. Many research papers and articles explored security issues as a hindrance in the adoption of IoT. IoT has already become a major security concern and various leading technology companies and governments across the globe are striving to find the right solution to this problem (Davis, 2020).

With the rapid increase in IoT application use, several security issues have raised sharply (Aldowah, 2019). However, other factors can slow down the progress of adoption of IoT which were not studied sufficiently to know the influence on IoT adoption. These factors are performance expectancy, facilitating conditions, effort expectancy explored in UTAUT. These factors play a

significant role in the adoption of any technology and are explored in detail in this research. The study will explore these three factors over security threats awareness and reveal the actual reasons which are influencing user intention to adopt IoT in the manufacturing industry. The extended UTAUT will be explored using a survey. The original four UTAUT constructs will be measured using the extant UTAUT instrument to preserve validity (Harper, 2016). The UTAUT model is extended by adding a security construct to understand the impact of security awareness on the adoption of IoT. Allen A. Harper used security as one of the constructs in his study. Following are the constructs which will be used for this study, security awareness, performance expectancy, effort expectancy, facilitating conditions. The other construct size of the company will also be taken into consideration for this study.

3.3 Research Questions and Hypothesis

Again, this study intends to build an extended technology adoption model for IoT in the manufacturing industry. There are primarily two types of questions that will support this study. The first question is, the influence of security awareness on consumer intention to adopt the IoT in the manufacturing industry, and the second question reveals other reasons which can influence consumer intention to adopt the IoT that are mainly facilitating conditions, performance expectancy, and efforts expectancy. The study will also explore the impact of the size of the organization (Large, Medium, and Small) on these four factors. The primary and secondary research questions and hypothesis for these questions are as follows:

3.3.1 Primary Question

Security Awareness

IoT has great potential in large, medium, and small enterprises however security issues continue to the technology of the IoT has depleted its adoption. Left unchecked, security issues may have a chilling effect on user personal privacy, safety, and security (Roman, 2011), Therefore, the research problem addressed by this study is the negative impact security issues have on adopting the IoT (Atzori, 2010). The study will be quantifying the relationship between awareness of security issues and intention to adopt the IoT. The security awareness of large, medium, and small Manufacturing Enterprises will be measured through the questionnaire.

The primary research question for this topic is, to what extent, if any, does a consumer's level of security awareness (SA) influence a consumers' intention to adopt the IoT? The following hypotheses apply to this question:

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

The above hypothesis will also be tested by using the size of the company as a moderator to test if the size of the company can influence security awareness and adoption of IoT.

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

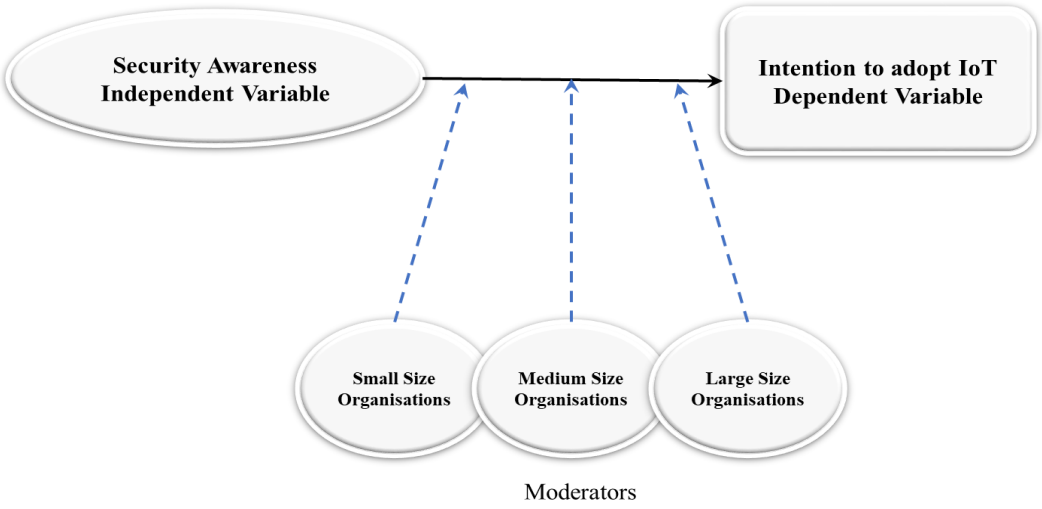

Figure 3-2: Research model for security awareness

3.3.2 Secondary Questions

Performance Expectancy

Performance expectancy is defined as the consumers' expectation that the use of IoT will improve performance. Performance Expectancy is drawn from other constructs, including the perceived usefulness of the Technology Acceptance Model also known as TAM (Davis, 1993). Performance expectancy was found to be the strongest predictor of behavioural intention to use technology (Venkatesh et al., 2003). This research will explore the relationship between performance expectancy and the intention to adopt IoT.

To what extent, if any, does consumers understanding of performance expectancy (PE) influences consumers' intention to adopt the IoT? The following hypotheses apply to this question:

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

The above hypothesis will also be checked by adding the size of the company as a moderator to understand the impact on performance expectancy and consumer intention to adopt IoT.

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

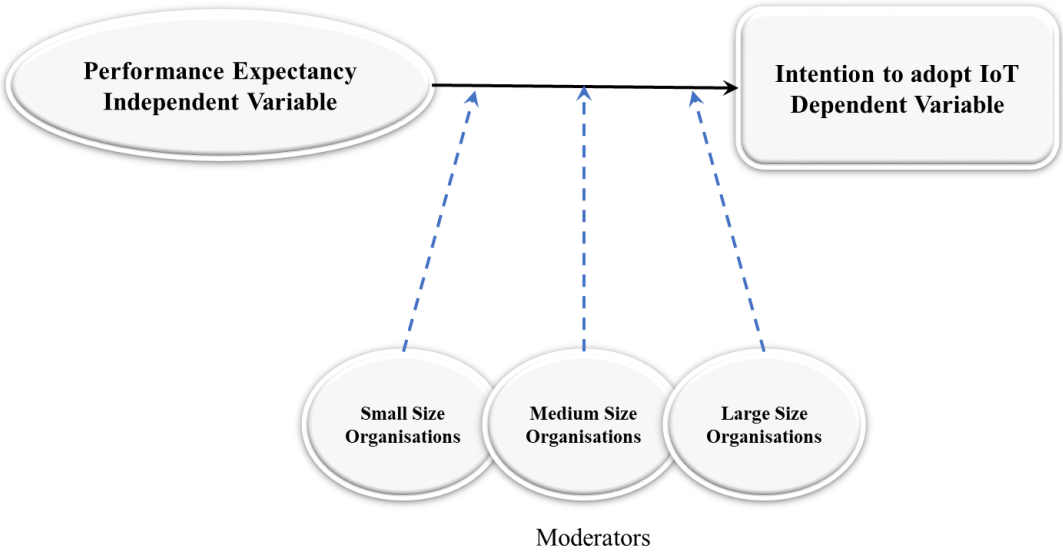

Figure 3-3: Research model of performance expectancy

Effort Expectancy

Effort Expectancy is defined as the measure of the perceived ease of use of the technology. Effort expectancy is also drawn from other constructs of other models, such as perceived ease of use of the TAM (Davis, 1993). The research will explore the relationship between effort expectancy and intention to use IoT.

To what extent Effort Expectancy impacts consumer intention to adopt the IoT.

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

This hypothesis will also be tested using the size of the company as a moderator to test if the size of the company can impact effort expectancy and adoption of IoT

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

.

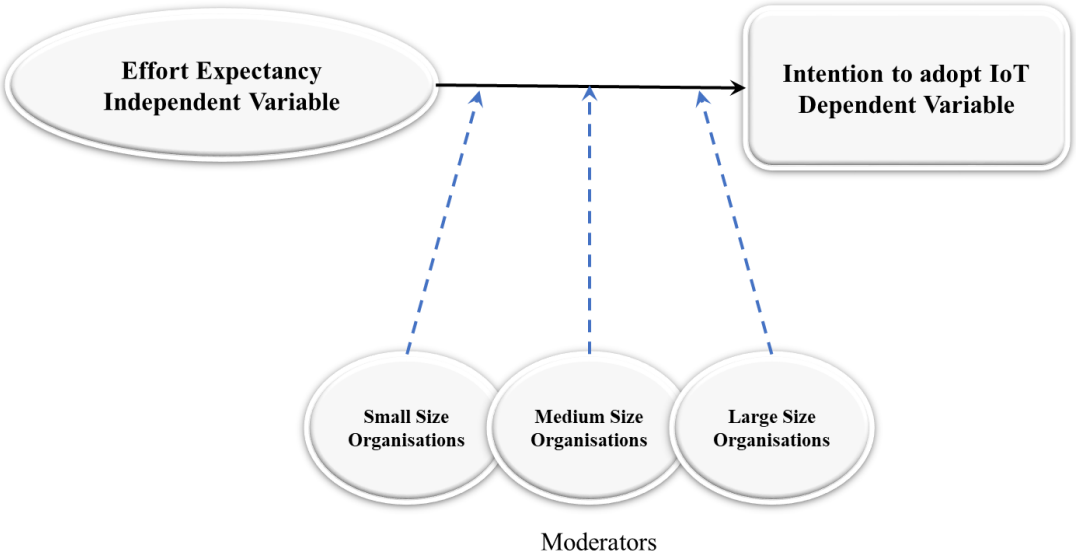

Figure 3-4: Research model of effort expectancy

Facilitating Conditions

Facilitating Conditions are defined as a collection of perceived infrastructures the user believes exists, to facilitate the use of the technology. As with the other constructs, the facilitating condition construct is derived from other models, including the innovation diffusion theory (IDT) of Moore

and Benbasat (1996). The research will explore the relationship between facilitating conditions and intention to use IoT.

To what extent facilitating conditions influence consumer intention to adopt the IoT.

$H_{4.0}$: Facilitating Conditions influences 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.

Like the above hypothesis, this one will also be tested by incorporating a moderator, organisation size. The moderator will test if the size of the company can moderate facilitating conditions relationship with consumer intention to adopt the IoT.

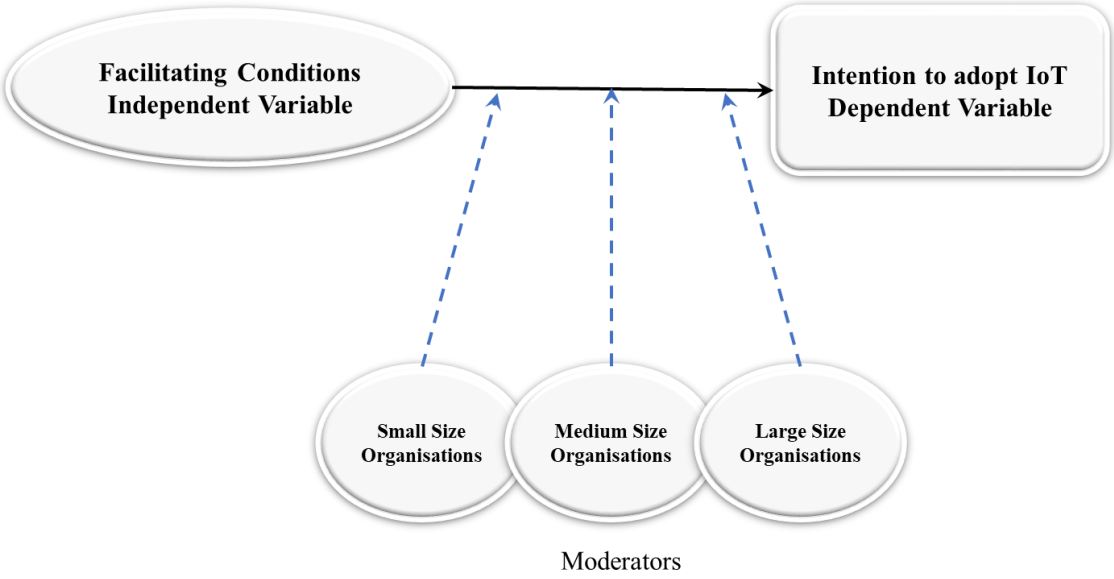

Figure 3-5: Research model of facilitating conditions

3.4 Methodological Approach

The most important methodological choice researchers make is between quantitative and qualitative data. Qualitative research involves the collection, analysis, and interpretation of non-numerical data like audio, videos, pictures, text, etc. It provisions a detailed understanding of the situation through data, but it is subjective. It involves a small sample of participants and findings are limited to the sample studied. The data interpretation cannot be generalized to the wider population.

On the other hand, quantitative research is the opposite of qualitative research. Quantitative methods are based on data that can be measured with numbers. The data is analysed on numerical comparisons and statistical analysis. Quantitative analysis requires numeric information in the form of variables. A variable is a way of measuring any characteristic that varies or has two or more possible values (Statistics Solutions, 2021).

As this research is based on data collection through a survey that can be converted into numbers for analysis, the quantitative method is chosen for data interpretation.

3.5 Target Population

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. Several private companies also provide such data.

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.

3.6 Questionnaire Design

In this study, data is collected from participants through the questionnaire. As a questionnaire is the most convenient and effective method to collect data from a large population, hence it is chosen for this study. A series of statements are designed for each variable. Each statement has multiple choice answers ranging from strongly agree to strongly disagree. The survey questions are designed in simple language which is understandable to the respondents. The survey document is formatted in a way to ensure content is conveyed to participants. Care is taken to avoid repeated questions to not lose respondents' interest.

Total 44 statements are designed for the survey. Out of 44, 26 questions are associated with constructs and 17 questions are generic to capture more information like name, email address, age etc			
. Variable	**Construct**	**No. of questions**	**Reference**
Dependent	Intention to adopt IoT	5	Adapted from Venkatesh and Davis (2000), Venkatesh et al. (2003),
Dependent	Awareness of IoT	2	NA
Independent	Security Awareness	5	Adapted from Harper, A. A. (2016, October)
Independent	Performance Expectancy	6	User acceptance of information technology: A unified view Venkatesh, Viswanath ProQuest Dissertations and Theses; 1998; ABI/INFORM Global
Independent	Effort Expectancy	4	Perceived ease of use, Davis 1989 and Moore and Benbasat, 1991
Independent	Facilitating conditions	4	User acceptance of information technology: A unified view Venkatesh, Viswanath ProQuest Dissertations and Theses; 1998; ABI/INFORM Global
NA	NA	18	Generic questions
Total		**44**	

Table 3-1: Questionnaire design and references

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

Table 3-2: Likert Scale

3.7 Pilot Study

A pilot study is also known as the "pre-study" of the final study. You may limit it by using fewer subjects than you plan to include in the full study, or you may limit it because your scope is smaller in some other way; for example, the range of types of subjects may be more limited (e.g., you use only undergraduates in the pilot when you plan to use a broader range of the general population in the full study) or the procedures may be more limited (e.g., you test people on their ability to recall a certain kind of word when in the full study you plan to examine people's ability to recall a greater range of words) (Woken, 2013). Some of the advantages of the pilot study are :

It helps to test all hypothesis in advance and allow to include relevant hypothesis for the full study. It helps to explore new ideas that researchers might have missed before the pilot run. It gives an overview of planned statistical and analytical producers along with the methodology used to understand the usefulness of the study. The pilot study reveals many undiscovered problems which help in redesign parts of the study to overcome the challenges of the final study. A sincere pilot study always provides enough data and overview to researchers to decide the usefulness of the study and whether to go for it or not. The main objective of the pilot study is to find out if questionnaire is measuring what it is supposed to (hence, reliability and validity checks), whether respondent could understand the questions and so on. The focus on pilot study is research instrument and hence, extensive tests on pilot is avoided due to small sample size which might not meet prerequisite of statistical tests. E.g. small sample sizes results in low power of regression tests.

To execute the pilot study, a survey was conducted, and data is collected from 50 entrepreneurs and senior staff of manufacturing companies in and around Mumbai. The survey was designed to answer different questions to understand security awareness, facilitating conditions, performance expectancy, effort expectancy of IoT.

Subsequently, A quantitative non-experimental correlational study was designed with objective of checking data consistency, efficacy of the questionnaire and research instrument.

- ❖ Reliability test of the independent variable using Cronbach's alpha.
- ❖ Multicollinearity test for each independent variable through Variance Inflation (VIF)

The intention to adopt IoT is a dependent variable that is evaluated through a question. Performance expectancy, effort expectancy, and facilitating conditions are also checked through different statements in the survey.

3.8 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 sixty thousand approximately. The error of tolerance is 5%.

Using Slovin's formula, the need for sample size is four hundred approximately.

3.9 Description of Sample for Full Study

The target group of the research is the owner and senior management who are running large, small, and medium size manufacturing enterprises in and around Mumbai. The organization details and their financial information is taken from the Ministry of Micro Small and Medium Enterprises (MSME) office in Delhi. The MSME gave the first level of information about the organization like organization name, authorized capital, paid-up capital, registrar of the company, principal business, and activation status. There are 3,54,932 records for PAN India received from the Ministry of MSME as depicted in table below.

Organisation Status	Count
Active	233596
Active in Progress	43
Amalgamated	5740
Captured	7
Converted to LLP	2247
Converted to LLP and dissolved	1753
Dissolved	5817
Dormant	7
Dormant under section 455	168
Liquidated	517
Not Available for eFiling	3394
Strike Off	96005
Under liquidation	1648
Under Process of Striking off	3990
Grand Total	**354932**

Table 3-3: Organization information from MSME

The information received from the Ministry of MSME was further refined to get data for companies that are active, registered in and around Mumbai and their principal business is manufacturing. There were 40, 737 records filtered which were relevant for this study as shown in table below.

Principal Business	Count
Manufacturing (Food stuffs)	3729
Manufacturing (Leather & products thereof)	275
Manufacturing (Machinery & Equipment)	9531
Manufacturing (Metals & Chemicals, and products thereof)	15818
Manufacturing (Others)	2523
Manufacturing (Paper & Paper products)	2613
Manufacturing (Textiles)	5947
Manufacturing (Wood Products)	301
Grand Total	**40737**

Table 3-4: MSME data for manufacturing organizations registered in Mumbai

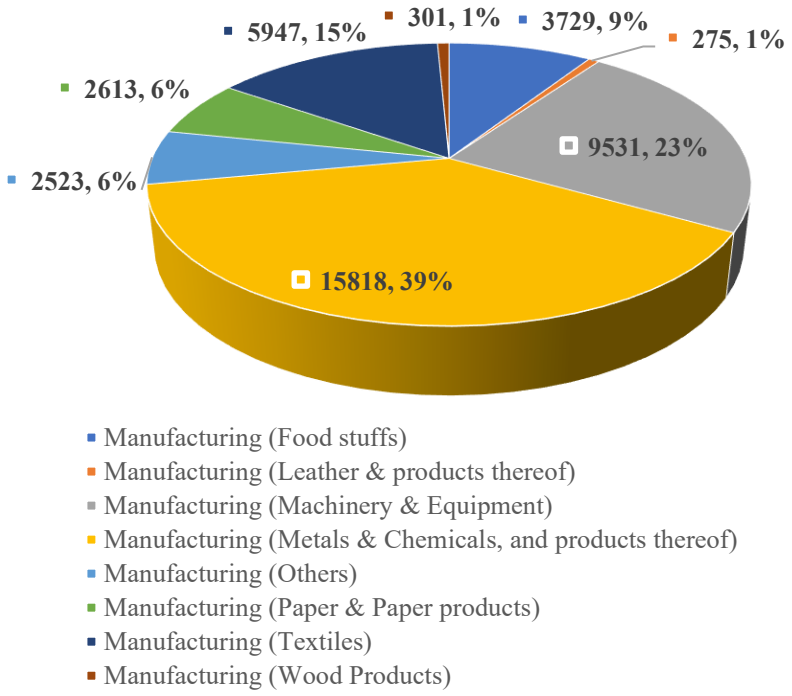

Figure 3-6:MSME data for manufacturing organisations in Mumbai

Slovin's guidelines are used to calculate the size of the sample. As per guidelines, 400 is the appropriate size of samples for the population of 40,737.

$N= 40737/[1+40737*.05^2] = 396$

Seven hundred manufacturing companies were identified to collect samples and simple random sampling method is used. The sample records were taken proportionally from industries and size of the organisation for each industry. The records were picked randomly through an online software (randomizer.org). The contact details of owners, senior management, and information technology head were collected through different internet sites and social media sites. Out of 700, 600 people were contacted through phone and face to face interview to answer the survey statements. The responses were received from 500 users. The records with incomplete information were removed and 423 records were validated for analysis as shown in the table.

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**

Table 3-5:Survey records

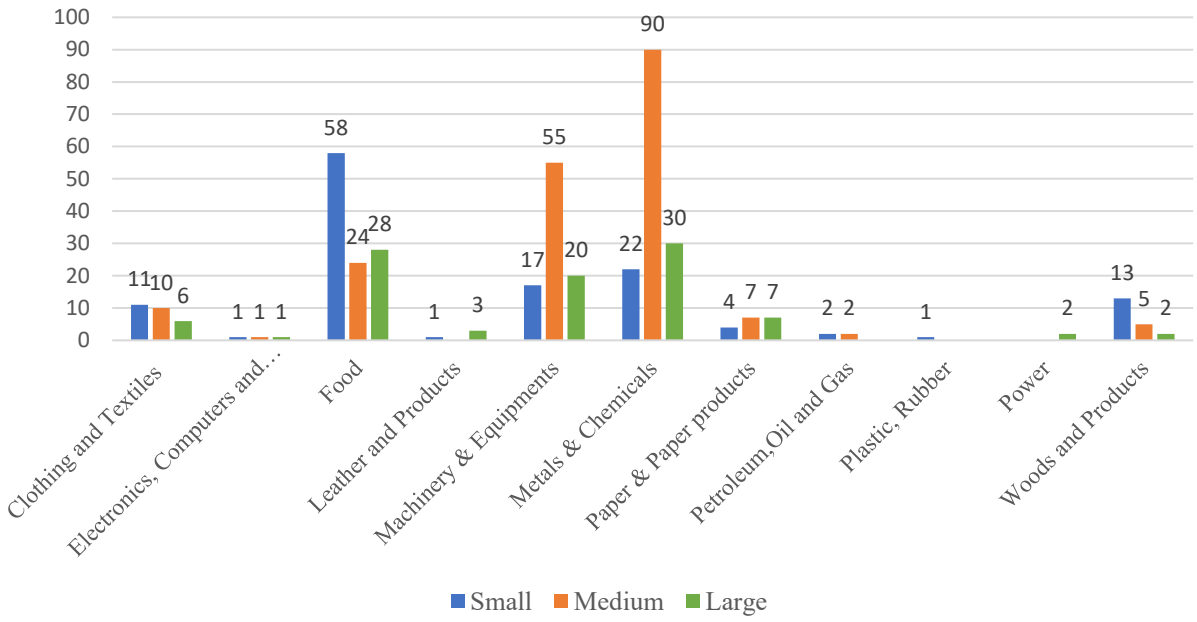

Figure 3-7: Graphical presentation of survey records

3.10 Data Collection

The data is collected through statements designed in questionnaire 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 supporting data that is organisation financial status and number of employees are collected through the Ministry of MSME, third parties and through websites. The supporting data is also verified during interviews where participants were ready to share information.

3.11 Data Analysis

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 will be used to show the relationship between different constructs.

Data will 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.

3.11.1 Rational for choosing correlational method

Correlational research is a type of research method that involves observing two variables to establish a relationship between them. Correlational research aims to identify variables that have some sort of relationship to the extent that a change in one creates some change in the other (Formplus, 2004). In this study, IoT adoption is a dependent variable that has a relationship with independent variables, awareness of security threats, facilitating conditions, performance expectancy and effort expectancy. The study will analyse the impact of change in values of each independent variable on the dependent variable. Hence, a correlational study is the most accurate method for this research. A similar approach is used by Cephus K. Nyandoro in his study in factors influencing ICT acceptance and use in small and medium enterprises in Kenya. The study used correlation approaches to answer the research questions. The correlation was relevant to the current study because they elucidated the contribution of previous researchers and put it in the appropriate context of overall knowledge (Nyandoro, 2016).

3.11.2 Rational for not performing consistency check for dependent variable

There are theories that disqualified that data consistency check for the large sample size. The central limit theorem (CLT) by Abraham de Moivre in 1733 explained, if sample sizes equal to or greater than thirty, it considered sufficient. It means, the distribution of the sample means is

normally distributed. Hence, the larger samples size, the more the graphed results take the shape of a normal distribution (Ganti, 2021). In a large sample size, the data is considered accurate whether the distribution is normal or anomalous.

3.11.3 Rational for Cronbach's alpha test

Cronbach's alpha which is also known as coefficient alpha is developed by Lee Cronbach in 1951 (Cronbach, 2004). It is used to measures reliability or internal consistency. It is used to test if multiple questions on the Likert scale are reliable or not. Internal consistency states that all questions on a scale or test contribute positively to measure the same construct. Cronbach's alpha, also known as coefficient alpha, is a measure of reliability, specifically internal consistency reliability or item interrelatedness, of a scale or test (e.g., questionnaire) (Howard, 1951).

The thumb rule for interpreting Cronbach's alpha for survey questions having multiple answers is as follows (Glen., 2021).

Cronbach's Alpha Test Results	**Consistency**
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

Table 3-6: Cronbach's Alpha result interpretation (Glen., 2021)

In this study Cronbach's alpha test is used to check the consistency among multiple questions asked through Likert survey for each independent variable.

3.11.4 Rational for Multicollinearity test

Multicollinearity is used to check the correlation between one or more independent variables. Multicollinearity occurs when two or more independent variables are highly correlated with one another in a regression model (Bhandari, 2020). This means one independent variable can be predicted from another independent variable. There are different ways to test multicollinearity like Variation Inflation Factor (VIF), correlation matrix, or correlation plot. VIF is suggested to be most suitable for testing one independent variable with a group of other independent variables. A correlation plot can be used to identify the correlation or bivariate relationship between two independent variables whereas VIF is used to identify the correlation of one independent variable with a group of other variables (Pulagam, 2020).

The thumb rule for interpretation of multicollinearity results using IVF by Stephanie Glen is (Glen, 2015) as follows:

VIF Value	Correlation
1	No Correlation
2 to 5	Moderate Correlation
>5	High Correlation

Table 3-7:VIF value interpretation *(Glen, 2015)*

In this study VIF is used to check the correlation among all independent variables.

3.11.5 Rational for Multiple Regression test

Multiple regression is used to predict the value of one variable based on the value of one or more variables. Multiple regression analysis allows researchers to assess the strength of the relationship between an outcome (the dependent variable) and several predictor variables as well as the importance of each of the predictors to the relationship, often with the effect of other predictors statistically eliminated (Petchko, 2018)

The last stage of data analysis is the multiple regression test of all independent variables with the dependent variable. The P-value extracted from the test shows the relationship between an independent variable and a dependent variable. P-values and coefficients in regression analysis work together to tell you which relationships in your model are statistically significant and the nature of those relationships (Frost, 2021). The coefficient describes the relationship between the independent variable and dependent variable which means, change in the value of an independent

variable will change the value of the dependent variable. The P-value explains whether this relationship is significant or not.

Before final analysis, it's important to establish a significance level which is the possibility of rejecting the null hypothesis when it is true. The significance level of 0.05 is statistically accepted by many researchers and the same will be used for this study. It indicates a 5% risk of concluding that a difference exists when there is no actual difference. Lower significance levels show it requires stronger evidence to reject the null hypothesis.

3.12 Conclusion, Recommendation and Future Research

The final stage of this study is sharing conclusions derived from data analysis and giving suitable recommendations for IoT service providers, academic institutions, government, and regulatory bodies to improve the adoption of IoT. The research will also provide avenues for researchers to further explore this study and apply this study to different industries.

3.13 Summary

This chapter covers, the purpose of the study. The gap which was found in other studies is elaborated like security awareness is given emphasis which hinders the adoption of IoT. However, other factors proposed in the Unified Theory of Acceptance and Use of Technology (UTAUT) are not explored. Thereafter, the questions and hypothesis for this study, security awareness, performance expectancy, effort expectancy, facilitating conditions are explained in detail. The quantitative and qualitative methods of research are elucidated. As this research is based on data collection through surveys, the quantitative method is chosen for data

interpretation. After explaining the method used for this study, the research design is explicated. The rationales are provided for choosing different tests for normality, reliability, multicollinearity, and multiple regression. Further, the population selected for the survey and sample size is described. After data collection, data analysis method is described. The chapter ended with description of conclusion, recommendation and future research that will be outcome of this study.

CHAPTER 4:
DATA ANALYSIS AND INTERPRETATION

CHAPTER 4: DATA ANALYSIS AND INTERPRETATION

4.1 Background

To this point, the topic and purpose of the study are explained. The gaps in other studies and literature are described. It is highlighted that a consolidated approach to evaluate the reasons that are impacting the users' intention to adopt IoT is found missing which will be covered in this study. The available models for technology adoptions are discussed. The UAUTA is the most recommended model by many researchers and adopted for this study too. Three constructs performance expectancy, effort expectancy, and facilitating conditions are taken from the UAUTA model. The security awareness is added as another construct to understand different criteria of adoption of IoT in manufacturing companies in and around Mumbai. Further, the impact of the size of the organisation is taken as an additional construct to understand if organisation size moderates relationship between independent and dependent variables. This chapter is throwing light on the pilot study conducted, its results, and interpretation. Thereafter, regression tests on data for the main study will be discussed. The results of the main study will be presented in this chapter and its interpretation will be discussed in the chapter 5.

4.2 Pilot Study Execution

As described in chapter 3, pilot study is conducted on 50 users. Data is collected through 5-point Likert survey questionnaire having multiple questions against each variable used in the study. After data collection, reliability test of the independent variable executed using Cronbach's alpha. The

multicollinearity test for each independent variable was also executed through Variance Inflation Factor.

4.2.1 Cronbach's Alpha Test

The Cronbach Alpha test is used here to check the reliability of independent variables which are security awareness, performance expectancy, effort expectancy, and facilitating conditions.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.991	0.992	5

Table 4-1:Security awareness reliability statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.977	0.978	6

Table 4-2:Performance expectancy reliability statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.996	0.996	4

Table 4-3:Effort expectancy reliability statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.947	0.945	5

Table 4-4:Facilitating condition reliability statistics

The tables show the Cronbach's Alpha test for security awareness, performance expectancy, effort expectancy, and facilitating conditions. As depicted in chapter 3, the Cronbach alpha greater than .9 is excellent and shows multiple questions asked for independent variables are internally consistent. In the above tests, all these results are greater than .9 which concludes the reliability of four independent variables.

4.2.2 Multicollinearity Test

After checking the reliability of each independent variable's questions, the multicollinearity check is performed to check the correlation among independent variables. The below tables depict the result of the multicollinearity test of security awareness, performance expectancy, effort expectancy, and facilitating conditions.

Coefficients[a]

Model		Collinearity Statistics
		VIF
1	(Constant)	
	Performance Expectancy	1.533
	Effort Expectancy	5.440
	Facilitating Conditions	5.987

a. Dependent Variable: Security Awareness

Table 4-5:Multicollinearity test for security awareness vs other variables (Pilot)

Coefficients[a]

Model		Collinearity Statistics
		VIF
1	(Constant)	
	Security Awareness	1.046
	Effort Expectancy	5.604
	Facilitating Conditions	5.681

a. Dependent Variable: Performance Eexpectancy

Table 4-6:Multicollinearity test for Performance Expectancy vs other variables (Pilot)

Coefficients[a]

Model		Collinearity Statistics
		VIF
1	(Constant)	
	Security Awareness	1.068
	Facilitating Conditions	1.534
	Performance Expectancy	1.613

a. Dependent Variable: Effort Expectancy

Table 4-7:Multicollinearity test for Effort Expectancy vs other variables (Pilot)

Coefficients[a]

Model		Collinearity Statistics
		VIF
1	(Constant)	
	Security Awareness	1.082
	Performance Expectancy	1.505
	Effort Expectancy	1.412

a. Dependent Variable: Facilitating Conditions

Table 4-8:Multicollinearity test facilitating conditions vs other variables (Pilot)

As shown in chapter 3, the VIF value 1 shows no correlation, the value from 2 to 5 shows moderate correlation, and a value greater than 5 is a high correlation. The above tables show most of the VIF values are in the range of 1 to 5 which prove moderate correlation among independent variables. Effort expectancy and facilitating conditions are marginally higher than 5 and considered to be moderately correlated.

4.3 Conclusion of Pilot Study

The primary purpose of this pilot study was to check research methodology design, effectiveness of questionnaire and can user interpret questions to give accurate answers to avoid ambiguity in data collection. The Cronbach's alpha test proved that multiple questions mentioned for each independent variable are reliable. The multicollinearity test results show low correlation among independent variables. There is moderate correlation among few independent variables which is

statistically accepted for this study. The practical experience during survey shows that users were able to understand questions and very comfortable answering it.

4.4 Main Study Execution

4.4.1 Demographic Analysis

		Numbers	%
Gender	Male	388	92%
	Female	35	8%
Age	26 to 35 Years	50	12%
	36 to 45 Years	181	43%
	46 to 55 Years	172	41%
	56 and above years	20	5%
Education	Graduation and Below	336	79%
	Post-Graduation and Above	87	21%

Table 4-9: Demographic Analysis

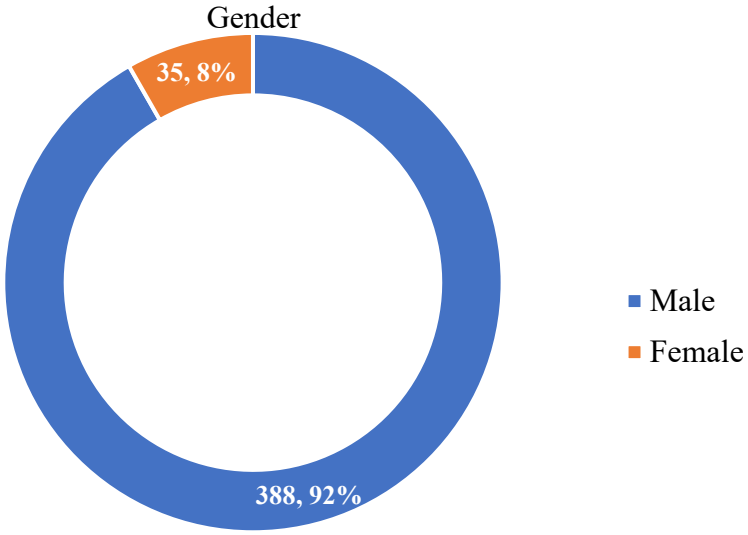

Figure 4-1: Demographic Analysis - Gender

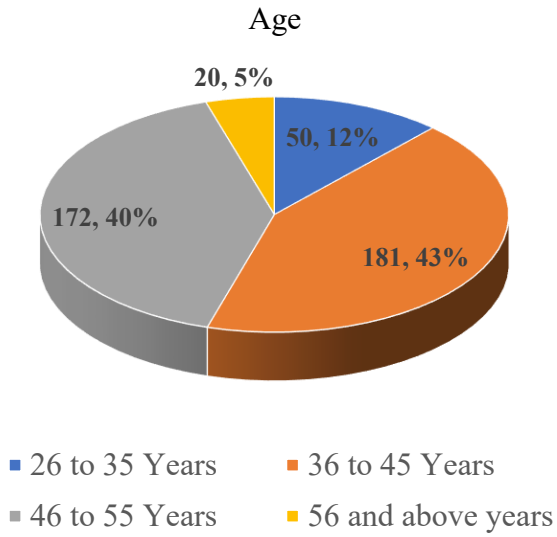

Figure 4-2:Demographic Analysis- Age

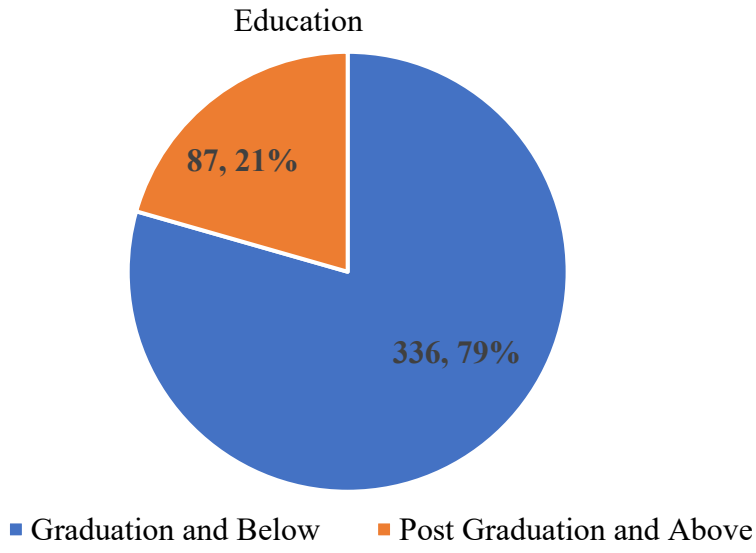

Figure 4-3: Demographic Analysis - Education

Interpretation:

The final population for data analysis is 423. The 388(92%) are male candidates and 35 (8%) candidates are female.

Out of 423, 50(12%) candidates are in the age group of 26 to 35, 181 (43%) are in 36 to 45, 172 (40%) are in 46 to 55 and 20 (5%) are in last category that is 56 and above.

The 336(79%) candidates out of 423 who are in the education category of graduation and below and 87(21%) candidates are graduates and above.

4.4.2 Descriptive Analysis

Intention of Using IoT		
Questions	**Mean**	**STD Dev**
If I had access to IoT, I would have the intention of using it.	1.25	0.63
I will always try to use IoT for my business.	1.24	0.61
I think it will be worth it for me to adopt IoT when it's available.	1.27	0.68
Assuming I have access to use IoT for my business, I would use it	1.34	0.81
Given opportunity, resources, and knowledge, I would use IoT for my business	1.32	0.77

Table 4-10: Descriptive Analysis of Intention of Using IoT

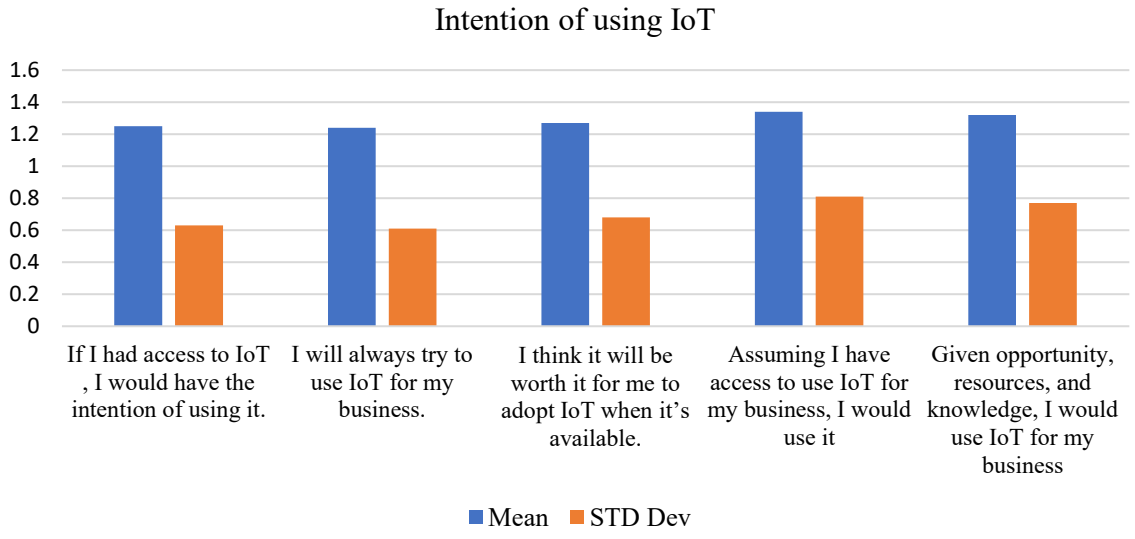

Figure 4-4: Descriptive Analysis of Intention of Using IoT

Interpretation:

The above table and graph infer that assuming I have access to use IoT for my business has highest mean (M=1.34, STD DeV=.81) followed by Given opportunity, resources, and knowledge, I would use IoT for my business (M=1.32 , STD DeV=.77) . Thereafter, I think it will be worth it for me to adopt IoT when it's available (M=1.27, STD DeV=.68) . If I had access to IoT , I would have the intention of using it (M=1.25 , STD DeV=.63) is second last and I will always try to use IoT for my business. (M=1.24 , STD DeV=.61) mean is the lowest.

Security Awareness		
Questions	**Mean**	**STD Dev**
I have threat to lose business data by using IoT.	3.54	1.181
I have threat from hackers who can access systems and impact business.	3.68	1.128
The business confidential information is not safe using IoT	3.52	1.185
The chances of virus and malware attack increase with use of IoT	3.58	1.179
The privacy is compromised using IoT	3.69	1.125

Table 4-11: Descriptive Analysis of Security Awareness

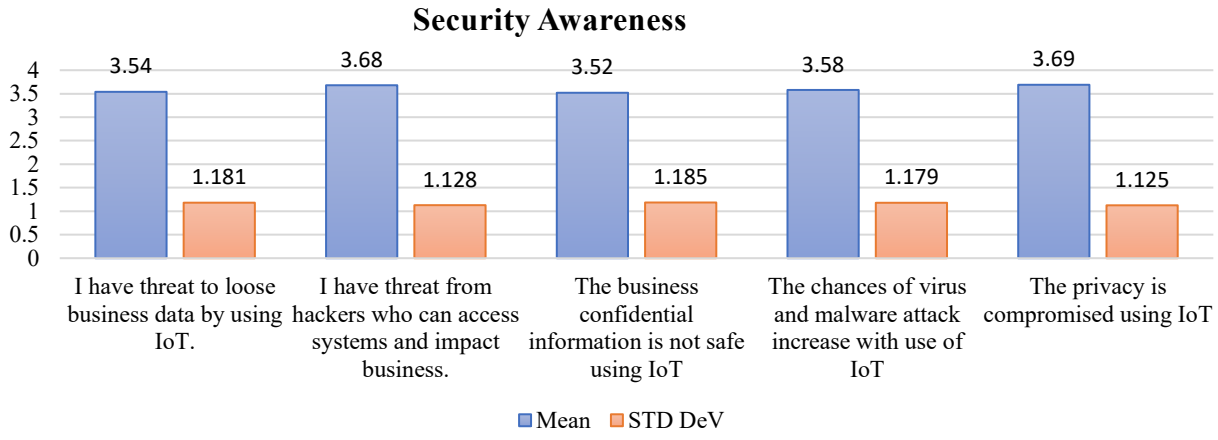

Figure 4-5: Descriptive Analysis of Security Awareness

Interpretation:

The above table and graph explain that construct privacy compromise has highest mean (M=3.69, STD DeV=1.125) followed by threat from hackers (M=3.68, STD DeV=1.128). Threat to lose data is third highest mean (M=3.54, STD Dev=1.181) and business confidential information safety has lowest mean (M=3.52, STD DeV= 1.185).

Performance Expectancy		
Questions	**Mean**	**STD Dev**
Using IoT in my job would enable me to accomplish task more quickly	2.05	0.801
Using IoT would make it easy to do my job	2.02	0.766
IoT improves the quality of work I do	2.2	0.916
Using IoT would increase my productivity	2.03	0.764
Use of IoT can decrease the time to do the important jobs	2.03	0.766
Use of IoT can improve the quality of output significantly	2.03	0.767

Table 4-12: Descriptive Analysis of performance Expectancy

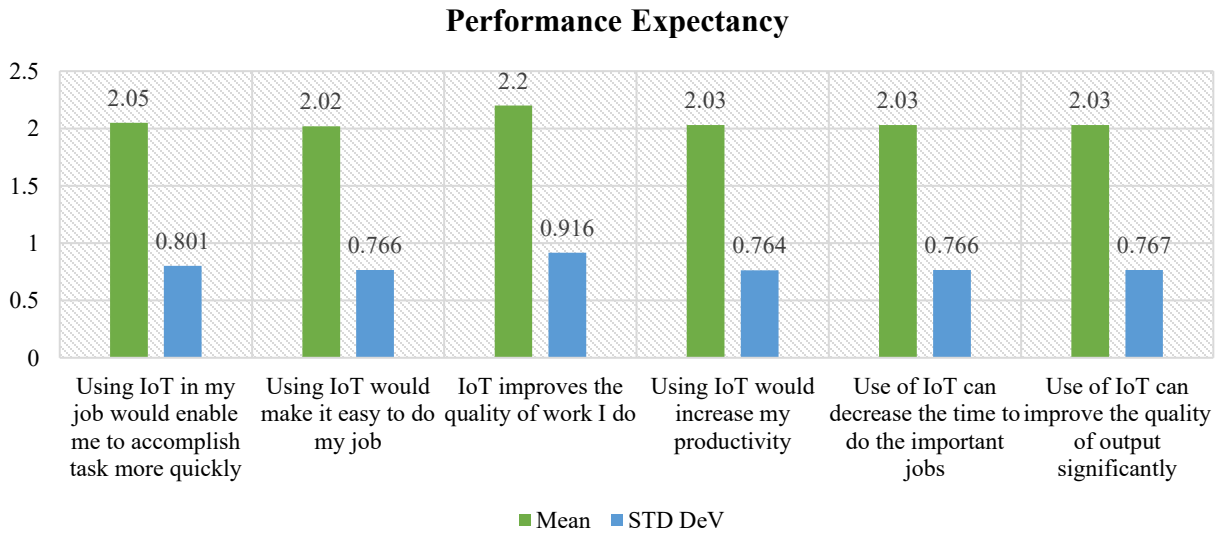

Figure 4-6: Descriptive Analysis of Performance Expectancy

Interpretation:

The table and graph decipher that IoT improves quality has the highest mean and standard deviation (M=2.2, STD DeV=0.916) followed by IoT enables to accomplish task quickly (M=2.05, STD DeV=0.801). There is less difference among mean and standard deviation of rest of the constructs, IoT would make it easy to do job (M=2.02, STD DeV=0.766), IoT would increase productivity (M=2.03, STD Dev=0.764), IoT decreases time to do job (M=2.03, STD Dev=0.766), IoT improves output quality (M=2.03, STD DeV= 0.767).

Effort Expectancy		
Questions	**Mean**	**STD Dev**
Learning how to use IoT for my business is easy for me.	2.19	0.873
My interaction with IoT is clear and understandable.	2.19	0.873
I find IoT easy to use.	2.19	0.874
It is easy for me to become skilful at using IoT.	2.2	0.888

Table 4-13: Descriptive Analysis of Effort Expectancy

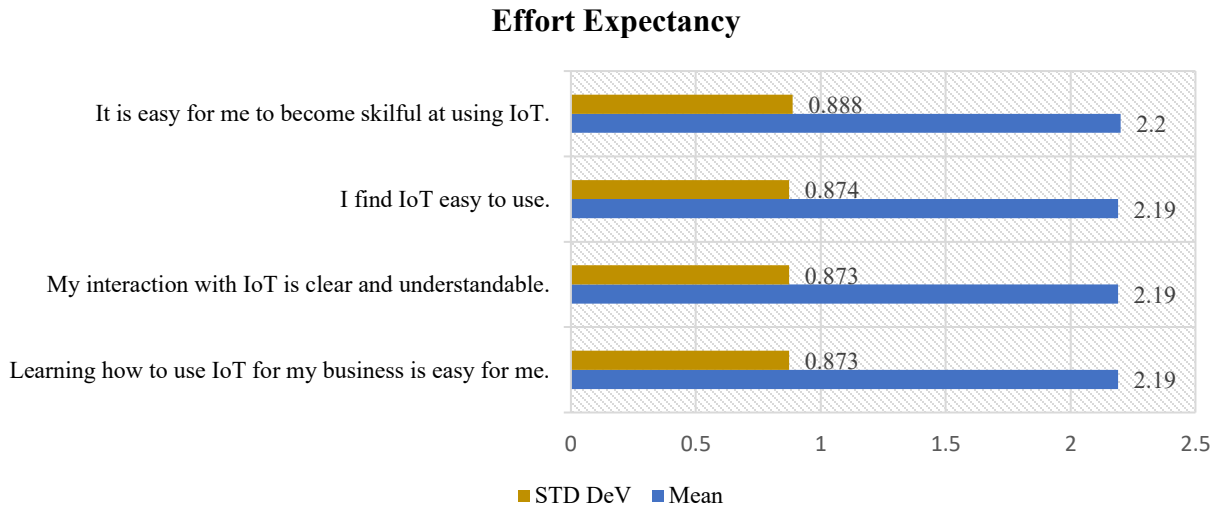

Figure 4-7: Descriptive Analysis Effort Analysis

Interpretation:

The descriptive analysis of effort expectancy table and graph shows that construct it's easy to become skilful has highest mean (M=2.2, STD DeV=.888). Rest of the constructs have same mean and STD DeV (M=2.19 and STD DeV=0.8).

Facilitating Condition		
Questions	**Mean**	**STD Dev**
I have the resources necessary to use IoT for my business	3.51	1.122
I have the knowledge necessary to use IoT for my business.	3.51	1.12
The IoT systems are compatible with other technologies I use.	3.51	1.118
I can get help from specialist people or group when I have difficulties using IoT	3.51	1.12
I got sufficient network bandwidth for connectivity	3.47	1.149

Table 4-14: Descriptive Analysis of Intention of facilitating Conditions

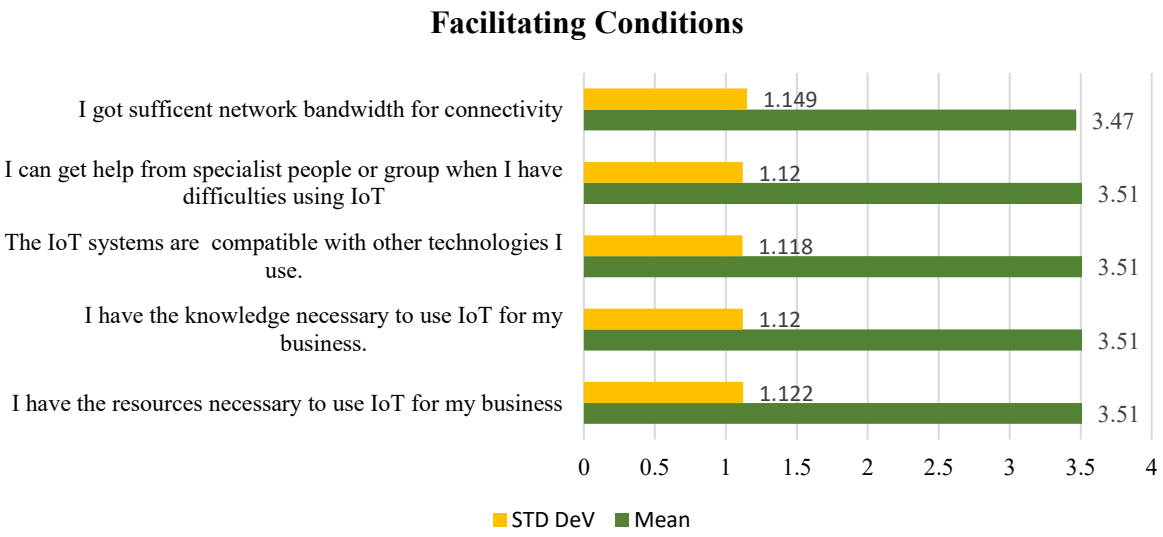

Figure 4-8:Descriptive Analysis of Facilitating Conditions

Interpretation:

The above table and graph show that mean and STD DeV for all constructs are similar. The construct helps from specialist, compatibility with other technologies, knowledge to use IoT,

necessary resources have same mean and approximate same standard deviation (M=3.51, STD DeV=1.1). Sufficient network bandwidth has somewhat lower mean (M=3.47, STD DeV=1.1).

4.5 Data Analysis

The data analysis was designed on the guidelines used for pilot study. These are

- Reliability test of each independent variable using **Cronbach's alpha.**
- Multicollinearity test for each independent variable through **Variance Inflation Factor (VIF).**
- Remove outliers from data through Inter Quartile Range (**IQR).**
- Run correlation between dependent and independent variables.
- Create Dummy Variables for large, medium, and small size organisations.
- Create interaction variables from organisation size and independent variables
- Run regression and ANOVA test

4.5.1 Reliability test of each independent variable

The Cronbach's alpha test is applied to measure reliability or internal consistency of independent variables. It testes if multiple questions on the Likert scale are reliable or not.

Cronbach's Alpha test for security awareness

Case Processing Summary

		N	%
Cases	Valid	423	100.0
	Excluded	0	.0
	Total	423	100.0

Table 4-15:Records Processed for security awareness Cronbach's Test

The above table shows all 423 records were processed for test.

Inter-Item Correlation Matrix

	Data Loss	Threat from Hacker	Confidential	Virus	Privacy
Data Loss	1.000	.878	.744	.816	.874
Threat from Hacker	.878	1.000	.851	.922	.996
Confidential	.744	.851	1.000	.766	.855
Virus	.816	.922	.766	1.000	.915
Privacy	.874	.996	.855	.915	1.000

Table 4-16:Inter-Item Correlation Matrix for security awareness

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.968	.969	5

Table 4-17:Cronbach's Test for security awareness

The tables show the correlation among five questions asked in the survey against the independent variable security awareness and result of Cronbach's test.

As described in chapter 3 about the interpretation of Cronbach's alpha test results, the α value greater than .9 is excellent, between .9 and .8 is good and between .8 and .7 is acceptable. As depicted the correlation values and Cronbach's alpha value are on the higher side which concludes there is no correlation among the five questions and independent viable is consistent. The Cronbach's Alpha result in table is greater than 9 which shows reliability of security awareness independent variable.

Cronbach's Alpha test for Performance Expectancy

The below tables show, all records are processed, and alpha values for correlation among six question of performance expectancy independent variable are on the higher side and there is no correlation among these questions. The Cronbach's Alpha test value is also greater than 9 and proves Performance Expectancy a reliable variable.

Case Processing Summary			
		N	%
Cases	Valid	423	100.0
	Excluded	0	.0
	Total	423	100.0

Table 4-18:Records Processed for PE Cronbach's Test

Inter-Item Correlation Matrix					
	Task Quickly	Easy to do job	Improve quality	Increase productivity	Decrease Time
Task Quickly	1.000	.909	.651	.907	.901
Easy to do job	.909	1.000	.729	.998	.992
Improve quality	.651	.729	1.000	.730	.728
Increase productivity	.907	.998	.730	1.000	.998
Decrease Time	.901	.992	.728	.998	1.000
Improve output	.899	.990	.729	.996	.998

Table 4-19:Inter-Item Correlation Matrix for Performance Expectancy

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.974	.977	6

Table 4-20: Cronbach's Alpha for Performance Expectancy

Cronbach's Alpha test for Effort Expectancy

In below table, it is shown that all 423 records are processed for Cronbach's alpha test to check the normality of independent variable effort expectancy.

Case Processing Summary			
		N	%
Cases	Valid	423	100.0
	Excluded	0	.0
	Total	423	100.0

Table 4-21:Records Processed for effort expectancy Cronbach's test

The correlation matrix shows high numbers which depict that there is no correlation among four questions of independent variable and Cronbach's Alpha value is greater than 9 that proves data is consistent and variable is reliable.

Inter-Item Correlation Matrix				
	Learn IoT	Interaction with IoT	Easy to use	Skills
Learn IoT	1.000	.998	1.000	.986
Interaction with IoT	.998	1.000	.998	.988
Easy to use	1.000	.998	1.000	.986
Skills	.986	.988	.986	1.000

Table 4-22:Inter-Item Correlation Matrix for Effort Expectancy

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.998	.998	4

Table 4-23: Cronbach's Alpha for Effort Expectancy

Cronbach's Alpha test for Facilitating Conditions

Similarly, table below shows that all records are processed and validated for Cronbach's alpha test for independent variable Facilitating conditions. The Cronbach's test shows the correlation among five questions of the independent variable and it depicts that there is no correlation among

five questions as numbers are very high. The value in Cronbach's Alpha test is greater than 9 that proves consistency of variable.

Case Processing Summary			
		N	%
Cases	Valid	423	100.0
	Excluded[a]	0	.0
	Total	423	100.0

Table 4-24:Records processed for facilitating condition Cronbach's test

Inter-Item Correlation Matrix					
	Resources	Knowledge	Compatibility	Specialist	Bandwidth
Resources	1.000	.996	.998	.999	.963
Knowledge	.996	1.000	.998	.999	.960
Compatibility	.998	.998	1.000	.999	.962
Specialist	.999	.999	.999	1.000	.962
Bandwidth	.963	.960	.962	.962	1.000

Table 4-25:Cronbach's test for facilitating conditions

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.997	.997	5

Table 4-26: Cronbach's Alpha for Facilitating Conditions

The Cronbach's alpha test performed for four independent variables security awareness, performance expectancy, effort expectancy and facilitating conditions describe low correlation among the questions asked for each independent variable. The high values of correlation matrix conclude that data is reliable and consistent. The Cronbach's Alpha tests performed on each variable show reliability of each independent variable

4.5.2 Multicollinearity test for each independent variable

After checking the correlation among different questions of the independent variable, it's important to test multicollinearity among independent variables. Multicollinearity occurs when two or more independent variables are highly correlated. The VIF is the most common and reliable way to measure multicollinearity as mention in chapter 3 and the same is followed in this study. The guidelines given by Stephanie Glen to interpret multicollinearity results using VIF are followed to interpret the results of the multicollinearity test. The VIF value of one indicates no correlation, the values from 2 to 5 shows moderate correlation and if the value is greater than 5, it means high correlation.

Security awareness correlation with other independent variables

The correlation table shows the Security Awareness correlation with performance expectancy, effort expectancy, and facilitating conditions. The table shows that the VIF value of security awareness with performance expectancy and effort expectancy is within the range of 2 to 5. Hence the correlation is moderate. The VIF value with facilitating condition is below 2 which indicates no correlation.

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	Performance Expectancy	.466	2.146
	Effort Expectancy	.424	2.357
	Facilitating Conditions	.943	1.060

a. Dependent Variable: Security Awareness

Table 4-27:Correlation test of Security Awareness Vs other variables

Performance expectancy correlation with other independent variables

The multicollinearity test of independent variable performance expectancy with other independent variables depicts in table below. The VIF values in the table show no correlation with effort expectancy, facilitating condition, and security awareness as the VIF value is below 2.

Coefficients[a]			
Model		Collinearity Statistics	
		Tolerance	VIF
1	Effort Expectancy	.835	1.197
	Facilitating Conditions	.942	1.062
	Security Awareness	.959	1.043

a. Dependent Variable: Performance Expectancy

Table 4-28:Correlation test of Performance Expectancy Vs Other Variables

Effort expectancy correlation with other independent variables

The correlation matrix of effort expectancy with facilitating condition, security awareness, and performance expectancy and the VIF results indicate no correlation of effort expectancy with other independent variables.

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	Facilitating Conditions	.948	1.055
	Security Awareness	.957	1.045
	Performance Expectancy	.915	1.092

a. Dependent Variable: Effort Expectancy

Table 4-29:Correlation test of Effort Expectancy Vs other variables

Facilitating condition correlation with other independent variables

The correlation of facilitating condition with security awareness, performance expectancy, and effort expectancy and VIF values show no correlation with security awareness as the VIF value is below 2. There is a moderate correlation with performance expectancy and effort expectancy as the VIF value is between 2 and 5.

Coefficients[a]			
Model		Collinearity Statistics	
		Tolerance	VIF
1	Security Awareness	.957	1.045
	Performance Expectancy	.464	2.154
	Effort Expectancy	.426	2.346

a. Dependent Variable: Facilitating Conditions

Table 4-30:Correlation test of Facilitating Conditions Vs other variables

The multicollinearity tests for one independent variable with other independent variables as depicted in tables show low VIF values which indicate no correlation among independent variables. This rejects the main hypothesis that there is a correlation among independent variables.

4.5.3 Remove outliers from data

Outlier data for dependent variable intention to adopt IoT

The IQR method is used to identify the outlier data and SPSS tool is used to identify 25th and 75th percentile. In the below table, the 25th percentile (Q1) is zero and 75th percentile (Q3) is one.

Percentiles						
		Percentiles				
		5	10	25	50	75
Weighted Average (Definition 1)	IoT Adoption	.00	.00	.00	1.00	1.00
Tukey's Hinges	IoT Adoption			.00	1.00	1.00

Table 4-31:Percentile for variable IoT adoption

IQR = Q3-Q1= 1-0=1

Lower Value = Q1-1.5*IQR = 0-1.5*1= **-1.5**

Any value which is below -1.5 is outlier.

Upper Value = Q3+1.5*IQR = 1+1.5*1= **2.5**

Any value above 2.5 will be outlier

The table below shows the extreme values of variable IoT Adoption and no value which is less than -1.5 and greater than 2.5. It indicates there is no outlier data to be remove.

Extreme Values				
			Case Number	Value
IoT Adoption	Highest	1	1	1
		2	2	1
		3	3	1
		4	5	1
		5	8	1[a]
	Lowest	1	422	0
		2	418	0
		3	417	0
		4	416	0
		5	415	0[b]

Table 4-32: Extreme values for variable IoT adoption

Outlier data for independent variable Security Awareness

The percentile table for SA shows 25th percentile (Q1) is 3 and 75th percentile(Q3) is 4.

Percentiles						
		Percentiles				
		5	10	25	50	75
Weighted Average (Definition 1)	SA	1.000000	2.000000	3.000000	4.000000	4.000000
Tukey's Hinges	SA			3.000000	4.000000	4.000000

Table 4-33: Percentile for variable Security Awareness (SA)

IQR= Q3-Q1= 4-3=1

Lower value = Q1-1.5*IQR= 3-1.5*1=**1.5**

Any value below 1.5 is outlier.

Upper value = Q3+1.5*IQR= 4+1.5*1=**5.5**

Any value above 5.5 is outlier.

The extreme value table shows the extreme values of variable security awareness. No value is less than 1.5 and above 5.5. hence, no records are outlier.

Extreme Values				
			Case Number	Value
SA	Highest	1	5	5.0000
		2	8	5.0000
		3	9	5.0000
		4	10	5.0000
		5	14	5.0000[a]
	Lowest	1	423	1.0000
		2	421	1.0000
		3	408	1.0000
		4	393	1.0000
		5	306	1.0000[b]

Table 4-34: Extreme values of variable Security Awareness (SA)

Outlier data for independent variable Performance Expectancy

The percentile table for independent variable Performance Expectancy and shows 25th percentile (Q1) is 2 and 7th percentile (Q3) is also 2.

IQR is 0 and upper and lower values are also 2. Any value which is lower and greater than 2 will be outlier.

Percentiles						
		Percentiles				
		5	10	25	50	75
Weighted Average (Definition 1)	PE	1.000000	1.000000	2.000000	2.000000	2.000000
Tukey's Hinges	PE			2.000000	2.000000	2.000000

Table 4-35: Percentile for variable Performance Expectancy (PE)

Table shows five records which are greater than 2 and five records are less than 2 and these records are outlier and to be removed.

Extreme Values				
			Case Number	Value
PE	Highest	1	142	5.0000
		2	253	5.0000
		3	36	4.0000
		4	134	4.0000
		5	145	4.0000[a]
	Lowest	1	423	1.0000
		2	421	1.0000
		3	416	1.0000
		4	415	1.0000
		5	414	1.0000[b]

Table 4-36: Extreme value for variable Performance Expectancy(PE)

Outlier data for independent variable Effort Expectancy

The percentile table shows the 25th percentile (Q1) of effort expectancy variable is 2 and 75th percentile (Q3) is also 2. This indicates the IQR is 0. As IQR is zero, the lower and upper values are 2. Hence, any value which is greater than 2 and less than 2 will be an outlier.

Percentiles							
		Percentiles					
		5	10	25	50	75	90
Weighted Average (Definition 1)	EE	1.000	1.000	2.000	2.000	2.000	4.000
Tukey's Hinges	EE			2.000	2.000	2.000	

Table 4-37:Percentile for variable Effort Expectancy (EE)

Table shows that there are five records which has value greater than 2 and five records has value less than 2. There records are outlier and to be removed from further study.

Extreme Values				
			Case Number	Value
EE	Highest	1	13	5.0
		2	142	5.0
		3	253	5.0
		4	279	5.0
		5	4	4.0[a]
	Lowest	1	423	1.0
		2	421	1.0
		3	416	1.0
		4	415	1.0
		5	414	1.0[b]

Table 4-38: Extreme value for variable Effort Expectancy (EE)

Outlier data for independent variable Facilitating Conditions

The below percentile table shows percentile for independent variable facilitating conditions. The 25^{th} percentile (Q1) is 3 and 75^{th} percentile (Q3) is 4.

Percentiles						
		Percentiles				
		5	10	25	50	75
Weighted Average (Definition 1)	FC	1.000000	2.000000	3.000000	4.000000	4.000000
Tukey's Hinges	FC			3.000000	4.000000	4.000000

Table 4-39: Percentile for variable Facilitating Condition (FC)

IQR= Q3-Q1= 4-3=1

Lower Value = Q1-1.5*IQR= 3-1.5*1=**1.5**

Upper Value = Q3+1.5*IQR = 4+1.5*1=**5.5**

Any value which is below 1.5 is outlier and value above 5.5 is also outlier.

The extreme value table depicts extreme upper and lower values of variable facilitating conditions and five records have a value less than 1.5 and no record which has a value greater than 5.5. The five records with a value of 1 are the outlier and to be removed.

Extreme Values				
			Case Number	Value
FC	Highest	1	13	5.0000
		2	19	5.0000
		3	55	5.0000
		4	57	5.0000
		5	61	5.0000[a]
	Lowest	1	421	1.0000
		2	413	1.0000
		3	412	1.0000
		4	411	1.0000
		5	387	1.0000[b]

Table 4-40: Extreme value for variable Facilitating Conditions (FC)

Outlier data for independent variable Organisation Size

Further, table below shows percentile for independent variable Organisation Size. The 25th percentile (Q1) is 1 and 75th percentile (Q3) is 2.

Percentiles						
		Percentiles				
		5	10	25	50	75
Weighted Average (Definition 1)	Org Size	1.00	1.00	1.00	2.00	2.00
Tukey's Hinges	Org Size			1.00	2.00	2.00

Table 4-41: Percentile for variable Organization Size

IQR= Q3-Q1= 2-1=1

Lower Value = Q1-1.5*IQR= 1-1.5*1=**-.5**

Upper Value = Q3+1.5*IQR = 2+1.5*1=**3.5**

Extreme Values				
			Case Number	Value
Org Size	Highest	1	4	3
		2	13	3
		3	16	3
		4	19	3
		5	46	3[a]
	Lowest	1	406	1
		2	405	1
		3	402	1
		4	401	1
		5	400	1[b]

Table 4-42: Extreme values for variable organization size

The extreme value table depicts no value in low range which are less than -.5 and above 3.5 in upper range.

The outlier exercise provided records that can be removed to improve the consistency of data for further analysis. There is no outlier data from the dependent variable IoT adoption. The security awareness has no record which is the outlier, the performance expectancy variable has ten outlier records, the effort expectancy variable has ten outlier records, facilitating condition has five outlier records, no outlier for Organisation Size. Some of the outlier records are common hence, in total 17 records are outlier:

36, 134, 142, 145, 253, 279, 376, 387,398, 401, 406,412, 413, 414, 415,416, 421

These records are removed from the data for further analysis.

4.5.4 Correlation between Dependent and Independent Variable

After removing outlier records the correlation test is run on 406 records where intention to adopt IoT is a dependent variable and security awareness, performance expectancy, effort expectancy, facilitating conditions are the independent variable.

Correlations – Independent Variable IU, Dependent Variables- SA, PE, EE, FC							
			IU	SA	PE	EE	FC
Spearman's rho	IU	Correlation Coefficient	1.000	.538**	.581**	.625**	.585**
		Sig. (2-tailed)	.	.000	.000	.000	.000
		N	406	406	406	406	406
	SA	Correlation Coefficient	.538**	1.000	.151**	.097	.152**
		Sig. (2-tailed)	.000	.	.002	.052	.002
		N	406	406	406	406	406
	PE	Correlation Coefficient	.581**	.151**	1.000	.719**	.176**
		Sig. (2-tailed)	.000	.002	.	.000	.000
		N	406	406	406	406	406
	EE	Correlation Coefficient	.625**	.097	.719**	1.000	.225**
		Sig. (2-tailed)	.000	.052	.000	.	.000
		N	406	406	406	406	406
	FC	Correlation Coefficient	.585**	.152**	.176**	.225**	1.000
		Sig. (2-tailed)	.000	.002	.000	.000	.
		N	406	406	406	406	406

**. Correlation is significant at the 0.01 level (2-tailed).

IU= Intention to adopt IoT, SA=Security Awareness, PE=Performance Expectancy, EE=Effort Expectancy, FC= Facilitating Conditions

Table 4-43: Correlation Matrix for SA, PE, EE and FC

The correlation matrix in the table shows the correlation of dependent variable intention to adopt IoT with independent variables security awareness, performance expectancy, effort expectancy, facilitating conditions. The correlation matrix shows higher numbers which proves correlation is significant between independent variable and dependent variable. In the table, the correlation between IU and SA is .538, IU and PE is .581, IU and EE is .625 and IU and FC is .585. All these values confirm moderately significant correlation (Patrick Schober, 2018).

4.5.5 Regression Test

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.932[a]	.869	.868	.2177784	.869	666.688	4	401	.000

a. Predictors: (Constant), Facilitating Conditions, Security Awareness, Performance Expectancy, Effort Expectancy

Table 4-44: Regression test

The R value of .932 in table explains fitment of model that is 93.2%.

The R-square value explains how close the data are to the fitted regression line. The definition of R-squared is the percentage of the response variable variation that is explained. The R square value 0% indicates that the model explains none of the variability of the response data around its mean and 100% indicates that the model explains all the variability of the response data around its

mean. In general, the higher the R-squared explains the model fits your data (Fisher, 1915). In the above table the R Square value is 86.9% which shows model fits the data.

Adjusted R-squared is a modified version of R-squared that has been adjusted for the number of predictors in the model. The adjusted R-squared increases when the new term improves the model more than would be expected by chance. It decreases when a predictor improves the model by less than expected. Typically, the adjusted R-squared is positive, not negative. It is always lower than the R-squared (Potters, 2021). In the above model the adjusted R Square value is 86.8% that proves goodness of the model.

The standard error of the estimate represents the average distance that the observed values fall from the regression line. It explains how wrong the regression model is on average using the units of the response variable. Smaller values are better because it indicates that the observations are closer to the fitted line (Frost, Statistics By Jim, 2021). The started error of the estimate in table is .217 which also very low.

The values of R square, Adjusted R Square and Standard Error of Estimate in table prove significance of the model.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.278	.050		5.590	.000	.180	.375
	SA	.220	.010	.392	21.428	.000	.200	.241
	PE	.287	.022	.346	12.849	.000	.243	.330
	EE	.220	.020	.305	11.218	.000	.181	.258
	FC	.205	.010	.372	19.793	.000	.185	.226

a. Dependent Variable: Intention of Using IoT

Table 4-45: Summary of Regression

Also, the significance value in the table above is zero which indicates the significance of all independent variables with dependent variable in the model.

Dummy Variables

To check if organisation size moderate other independent variables impact on user intention to adopt IoT, the dummy variables are created for large, medium, and small size organisations as organisation size is a categorical variable. Categorical variables require special attention in regression analysis because, unlike dichotomous or continuous variables, they cannot be entered into the regression equation just as they are. Instead, they need to be recoded into a series of variables which can then be entered into the regression model (UCLA, 2021).

Interaction Variable with Independent and Dummy Variables

To check the moderation of organization size on independent variable, the interaction variables are created using dummy variables for each size of the organization and independent variables as follows:

Interaction_SA*Small Dummy, Interaction_SA*Medium Dummy, Interaction_SA*Large Dummy, Interaction_PE*Small Dummy, Interaction_PE*Medium Dummy, Interaction_PE*Large Dummy, Interaction_EE*Small Dummy, Interaction_EE*Medium Dummy, Interaction_EE*Large Dummy, Interaction_FC*Small Dummy, Interaction_FC*Medium Dummy, Interaction_FC*Large Dummy.

4.6 Regression test for hypothesis

4.6.1 Research Question 1

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

Coefficients[a]

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
	Std. Error	Beta			Lower Bound	Upper Bound
SA	.010	.392	21.428	.000	.200	.241

a. Dependent Variable: Intention of using IoT

Table 4-46: Security Awareness Coefficients

The p value 0 proves statistically significance of Security Awareness and confirms its influence on consumer intention to adopt IoT. The unstandardised β value explains 22% influence of SA individually and standardise β value deciphers 39.2% influence collectively with other variables.

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

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.537[a]	.288	.283	.5075025

a. Predictors: (Constant), Interaction_SAxLargeDummy, Interaction_SAxSmallDummy, Interaction_SAxMediumDummy

Table 4-47:Summary - Interaction Variables Security Awareness & Organization Sizes

The R value of .537 shows moderate relationship between independent and dependent variables and R2 value explains the 28.8% of variance in dependent variables with change in independent variables collectively.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	41.957	3	13.986	54.301	.000[b]
	Residual	103.539	402	.258		
	Total	145.496	405			

a. Dependent Variable: Intention of using IoT
b. Predictors: (Constant), Interaction_SAxLargeDummy, Interaction_SAxSmallDummy, Interaction_SAxMediumDummy

Table 4-48: ANOVA Test-Interaction Variables Security Awareness & Organization Sizes

The p value of 0 explains statistically significance of model.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.816	.080		22.830	.000
	Interaction_SAxSmall Dummy	.312	.026	.825	11.903	.000
	Interaction_SaxMediu mDummy	.289	.025	.857	11.745	.000
	Interaction_SaxLargeD ummy	.237	.029	.547	8.284	.000

a. Dependent Variable: Intention of using IoT

Table 4-49:Coefficient -Interaction Variables Security Awareness & Organization Sizes

The p value is zero for each interaction variable and proves statistically significance of each independent variable. The unstandardised coefficient values shows low influence of independent variables individually while collectively influence is higher as standardised coefficient is higher.Unstandardised Coefficient (Interaction_SaxSmallDummy=.312,Interaction_SaxMediumDummy= .289, Interaction_SaxLargeDummy= .237). Standardised Coefficient (Interaction_SaxSmallDummy=.825,Interaction_SaxMediumDummy= .857, Interaction_SaxLargeDummy= .547).

4.6.2 Research Question 2

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

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	PE	.287	.022	.346	12.849	.000	.243	.330

a. Dependent Variable: Intention of using IoT

Table 4-50: Performance Expectancy Coefficients

The significance value of 0 proves statistically significance of the model. The unstandardised β value explains the 28.7% influence of performance expectancy independently and standardised value explains 34.6% influence of collectively.

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

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.698[a]	.488	.484	.4306078

a. Predictors: (Constant), Interaction_PExSmallDummy, Interaction_PExLargeDummy, Interaction_PExMediumDummy

Table 4-51:Summary- Interaction Variables Performance Expectancy & Organization Sizes

For further analysis to find if organisation size moderates Performance Expectancy, R value signifies 69.8% change of dependent variable with change in independent variable. The R2 implies 48.8% change in dependent variable with collective change of performance expectancy with other independent variables.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	70.956	3	23.652	127.556	.000[b]
	Residual	74.540	402	.185		
	Total	145.496	405			

a. Dependent Variable: Intention of using IoT

b. Predictors: (Constant), Interaction_PExSmallDummy, Interaction_PExLargeDummy, Interaction_PExMediumDummy

Table 4-52:ANOVA-Interaction Variables Performance Expectancy & Organization Sizes

The ANOVA table explains statistically significance of model having intention of using IoT as dependent variable and three interaction variables created with three size of organisations and Performance Expectancy.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.531	.067		23.010	.000
	Interaction_PExLargeDummy	.544	.039	.763	13.787	.000
	Interaction_PExMediumDummy	.572	.031	1.127	18.411	.000
	Interaction_PExSmallDummy	.583	.032	1.051	18.158	.000

a. Dependent Variable: Intention of using IoT

Table 4-53:Coefficient- Interaction Variables Performance Expectancy & Organization Sizes

The p value is 0 in the coefficient test for each interaction variable that explains statistically significance of each variable. The standardised β value explains moderate influence of interaction variable individually whereas standardised β values explains higher influence collectively. Unstandardised Coefficient (Interaction_PExSmallDummy=.583, Interaction_PExMediumDummy= .572, Interaction_PExLargeDummy= .544). Standardised Coefficient (Interaction_PExSmallDummy=1.051, Interaction_PExMediumDummy= 1.127, Interaction_PExLargeDummy= .763).

4.6.3 Research Question 3

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

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	EE	.220	.020	.305	11.218	.000	.181	.258

a. Dependent Variable: Intention of using IoT

Table 4-54: Effort Expectancy Coefficients

The p value 0 in coefficient table proves statistically significance of model. The standardised β value decipher 22% influence of Effort Expectancy individually and standardised β value interpret 30.5% influence collectively.

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

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.708[a]	.501	.497	.4250669

a. Predictors: (Constant), Interaction_EExLargeDummy, Interaction_EExSmallDummy, Interaction_EExMediumDummy

Table 4-55:Summary - Interaction Variables Effort Expectancy & Organization Sizes

In the model summary table, the R value of .708 explains 70.8% influence of model individually and R2 value of .501 interpret 50.1% influence collectively.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	72.861	3	24.287	134.419	.000[b]
	Residual	72.634	402	.181		
	Total	145.496	405			

a. Dependent Variable: Intention of using IoT
b. Predictors: (Constant), Interaction_EExLargeDummy, Interaction_EExSmallDummy, Interaction_EExMediumDummy

Table 4-56:ANOVA-For Interaction Variables Effort Expectancy & Organization Sizes

The ANOVA table decipher statistically significance of the model as p value is 0.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.580	.062		25.356	.000
	Interaction_EExSmallDummy	.487	.026	1.029	18.752	.000
	Interaction_EExMediumDummy	.549	.029	1.081	18.642	.000
	Interaction_EExLargeDummy	.502	.036	.732	13.997	.000

a. Dependent Variable: Intention of using IoT

Table 4-57:Coefficient Test-Interaction Variables Effort Expectancy & Organization Sizes

The above table explains significance of each interaction variable because the p value is 0. The unstandardised β value of interaction variables show moderate influence on dependent variable individually whereas the influence is higher collectively as standardised β values are higher.

4.6.4 Research Question 4

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

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	FC	.205	.010	.372	19.793	.000	.185	.226

a. Dependent Variable: Intention of using IoT

Table 4-58: Facilitating Conditions Coefficients

The p value 0 indicates statistically significance of the model. The unstandardised β value explains 20.5% influence of Facilitating Conditions independently whereas standardised β value decipher 37.2% influence collectively.

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

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.599[a]	.358	.354	.4818829

a. Predictors: (Constant), Interaction_FCxLargeDummy, Interaction_FCxSmallDummy, Interaction_FCxMediumDummy

Table 4-59:Summary - Interaction Variables Facilitating Conditions & Organization Sizes

The model summary table shows R value .599 that explains 59.9% of influence individually and R2 value is .358 that is 35.8% of influence collectively.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	52.147	3	17.382	74.855	.000[b]
	Residual	93.349	402	.232		
	Total	145.496	405			

a. Dependent Variable: Intention of using IoT

b. Predictors: (Constant), Interaction_FCxLargeDummy, Interaction_FCxSmallDummy, Interaction_FCxMediumDummy

Table 4-60:ANOVA- For Interaction Variables Facilitating Conditions & Organization Sizes

The p value is 0 in ANOVA table that shows statistically significance of model having Intention of using IoT as dependent variable and three interaction variables created with facilitating conditions and three size of dummy variables.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.719	.075		22.914	.000
	Interaction_FCxSmallDummy	.348	.025	.924	14.184	.000
	Interaction_FCxMediumDummy	.311	.023	.937	13.589	.000
	Interaction_FCxLargeDummy	.262	.027	.610	9.803	.000

a. Dependent Variable: Intention of using IoT

Table 4-61:Coefficient-Interaction Variables Facilitating Conditions & Organization Sizes

Further, the coefficient table explains low influence of interaction variables on consumer intention to adopt IoT individually because of low value of unstandardised β value whereas collectively its higher as standardised β value is higher.

4.7 Summary

The chapter starts with a pilot run for 50 samples. The pilot study design was explained. Thereafter Cronbach's alpha test and Multicollinearity test were performed to check independent variables' reliability. The pilot study section was concluded with result analysis of tests performed. The sample size for the main study was discussed. The execution of the reliability test for independent variables for main study was the next section. Afterwards, correlation and multiple regression was run followed by One-Way-Anova.

CHAPTER: 5
RESULT, DISCUSSIONS & CONCLUSIONS

CHAPTER 5: RESULTS, DISCUSSIONS AND CONCLUSIONS

Up to this stage, the study has furnished a problem statement, research topic, research questions accompanied by hypotheses for each problem. Subsequently, a literature review was provided on the topic. Then, the methodology used for a non-experimental study was explained. The sample size and source of sampling were discussed. Thereafter, the pilot run was performed on a sample of 50 records. After the pilot study, the test was performed for each hypothesis for full data. In Chapter 4, the results of the study were presented. In this chapter, a full discussion of the results will be provided. Next, conclusions will be drawn and implications of the study to others will be explored. Limitations will be discussed along with implications for practice. Finally, recommendations will be provided for areas of future study to contribute to the body of knowledge.

5.1 Summary of the Results

In chapter 4, a pilot study was conducted with a sample size of 50 participants of the survey and thereafter the main study was conducted on the sample size of 406 participants. The research method was chosen for the pilot as well as the main study was a quantitative, non-experimental, correlational study using regression as the form of data analysis.

The data analysis for the main study started with the reliability test of independent variables using Cronbach's alpha test. The Cronbach alpha test was run on the independent variables security awareness, performance expectancy, effort expectancy and facilitating conditions to check internal consistency. As described in chapter 3, the thumb rule is, if α greater than .9 is excellent, between .9 and .8 is good and between .8 and .7 is acceptable. The Cronbach's test tables show results either

greater than .9 or between .9 to .8. There are few cases where α is between .7 to .8. Hence, it concludes high consistency among survey questions for each independent variable.

Next, multicollinearity tests for independent variables are conducted to check if independent variables are correlated. Stephanie Glen's guidelines are followed to interpret multicollinearity test results. The VIF value of one indicates no correlation among independent variables, the values from 2 to 5 shows moderate correlation and if the value is greater than 5, it means high correlation. The VIF values in test results are between 1 to 3 which are on the lower side and concludes low correlation between independent variables.

Subsequently, outlier data is removed using the IQR method. The IQR was applied to the dependent variable and all independent variables. The outliers from respective variables were removed from the data. After building consistency in data, correlation and multiple regression was used to check the relationship between dependent and independent variables. The four independent variables were Security Awareness, Performance Expectancy, Effort Expectancy and Facilitating Conditions. Further, to check if organisation size moderates the impact of independent variable on dependent variable, interaction variables were built. Thereafter, regression test was executed with interaction variable and dependent variable.

5.2 Discussion of the Results

In this section, the results will be discussed for each research question.

5.2.1 Research Question 1

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

To test this hypothesis, a correlation was checked between Security Awareness independent variable and Intention to use IoT dependent variable. The significance value 0 proves significance of the model and correlation value .538 shows positive correlation between security awareness and intention to use IoT.

Thereafter, a regression test was performed to check the level of influence of security awareness on intention to adopt IoT and results shows the model is statistically significant as p value is 0 as well as standardise β (.392) and unstandardised β (.220) values prove the influence but it's not very high.

As above test validated the relationship between security awareness and intention to use IoT. Hence, main hypothesis is accepted and null hypothesis is rejected.

The next hypothesis is to verify if organisation size moderates this relationship.

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

The correlation test for organisation size influence on security awareness and intention to use IoT shows that small, medium and large size organisations moderate the relationship as p values for all variables are 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 size (.825) and medium size (.857) organisations is higher than interaction variable build with large size (.547) organisation.

The analysis supports mail hypothesis and rejects null hypothesis.

The analysis prove that security awareness has positive relationship with intention to adopt IoT. To further validates that small and medium size organisations moderates this relationship more than the large size organisation.

5.2.2 Research Question 2

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

Like above hypothesis the relationship between performance expectance and intention to use IoT is tested through correlation. The p value is 0 which justify the significance of the model statistically. The correlation value of .581 shows positive correlation between two variables.

To test the level of influence of performance expectancy on intention of using IoT, regression test was made. The p value is 0 which proves statistically significance of the model and standardised coefficient value of .346 indicates moderate level of influence of performance expectancy on intention to use IoT.

The analysis supports mail hypothesis and rejects null hypothesis.

To explore if organisation size moderates the relationship between two variables, further testes were made.

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

The correlation test results for organisation size influence on performance expectancy and intention to use IoT relationship explain significance of each interaction variables on intention to use IoT as p value is 0. The standardised values for interaction variable with large size organisation (.763), medium size organisation (1.127) and small size organisation (1.051) infer the strong influence of all size of the organisations on the relationship between performance expectancy and intention to use IoT. Hence, main hypothesis is accepted and null hypothesis is rejected.

The analysis deciphers the moderate relationship between performance expectancy and intention to use IoT. Further analysis proves all size of the organisations moderates the relationship between two variables.

5.2.3 Research Question 3

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

The p value of 0 in correlation test infers statistically significance of the model. The correlation value is .625 that proves positive correlation between effort expectancy and intention to use IoT.

To check the level of influence of effort expectancy on the intention to use IoT, a regression test was performed. The p value of 0 proves significance and standard coefficient value of .305 infers moderate level of influence of effort expectancy on intention to use IoT.

The analysis supports main hypothesis and rejects null hypothesis.

The next level of test is to check which size of the organisation moderates the relationship between effort expectancy and intention to use IoT.

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

The results of coefficient test for organisation size influence on effort expectancy and intention to use IoT relationship explains statistically significance as p value is 0. It also deciphers that all size of the organisations moderates the relationship between effort expectancy and intention to use IoT because standardised coefficient value of interaction variable with small size organisation is 1.029, medium size organisation is 1.081 and large size organisation is .732. Hence, the main hypothesis is accepted and null hypothesis is rejected.

The above analysis concludes that there is a relationship between effort expectancy and intention to use IoT and this relationship is moderated by large, medium and small size organisations significantly.

5.2.4 Research Question 4

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

The correlation test between facilitating conditions and intention to use IoT proves statistically significance as p value is 0. It also shows a positive relationship between two variables as correlation coefficient value is .585.

Thereafter, a regression test is performed to check the level of influence of facilitating conditions on the intention to adopt IoT. The results explain statistically significance of the model as p value is 0 and level of influence of facilitating condition is moderate as standardised coefficient value is .372. Hence, the main hypothesis is accepted and null hypothesis is rejected.

Further, test was performed to check if organisation size moderates the relationship between facilitating conditions and intention to adopt IoT and which size of the organisation influence.

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

A coefficient test was performed to test if organisation size moderates the relationship between two variables. The results explain statistically significance as p value is 0. It also shows influence of all size of the organisation on relationship between facilitating conditions and intention to adopt IoT because the value of interaction variable with small size organisation is .924, medium size organisation is .937 and large size organisation is .610.

The analysis supports the main hypothesis and rejects null hypothesis.

The above analysis concludes that facilitating condition has relationship with Intention to use IoT and large, medium and small size organisations moderate this relationship. The medium and small size organisation has strong influence while large size has moderate influence on relationship between independent and dependent variables.

5.3 Research Model

After discussing the result, the new model of the research is depicted in below figures. The model describes security awareness, performance expectancy, effort expectancy and facilitating conditions are statistically significant and have relationship with Intention to Adopt IoT. Similarly, the model created with interaction variable shows, each interaction variable is significant and have relationship with intention to Adopt IoT.

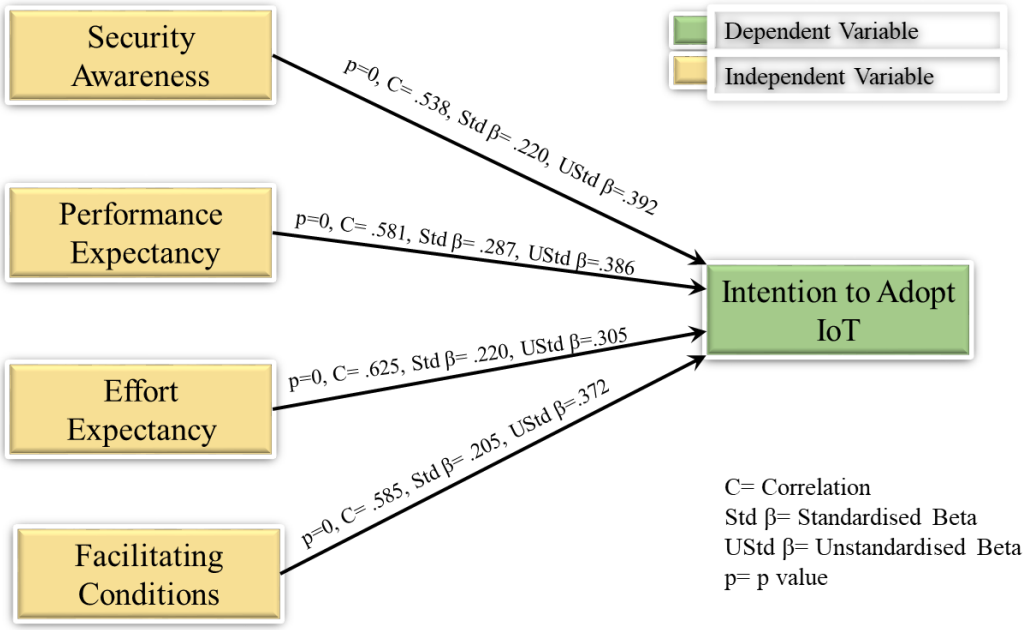

Figure 5-1: Research model Dependent and Independent Variables

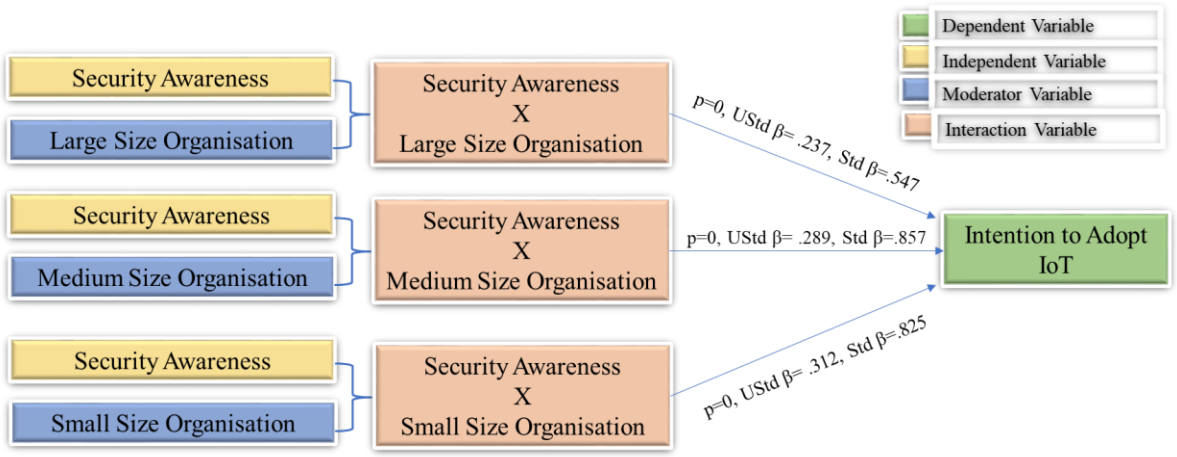

Figure 5-2: Model with interaction variable Security Awareness and Organization Size

Figure 5-3: Model with interaction variable Performance Expectancy and Organization Size

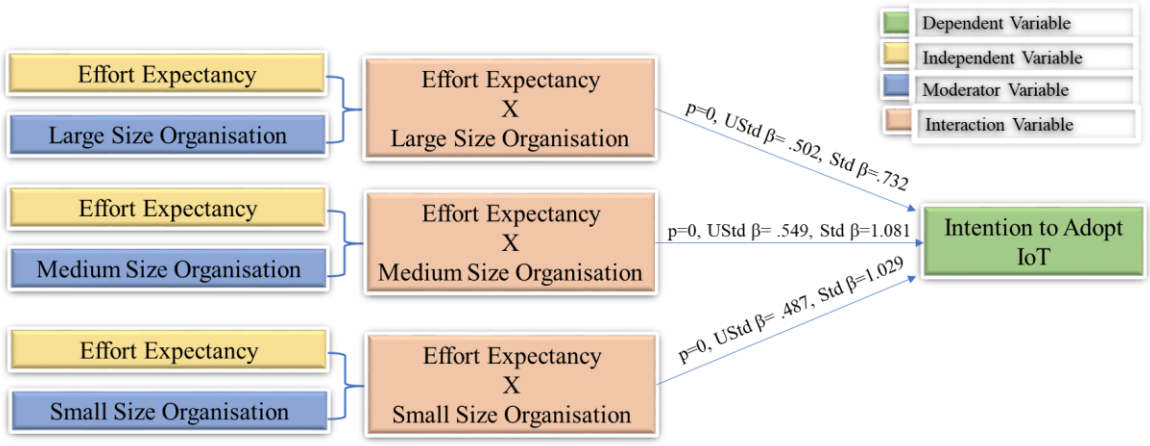

Figure 5-4: Model with interaction variable Effort Expectancy and Organization Size

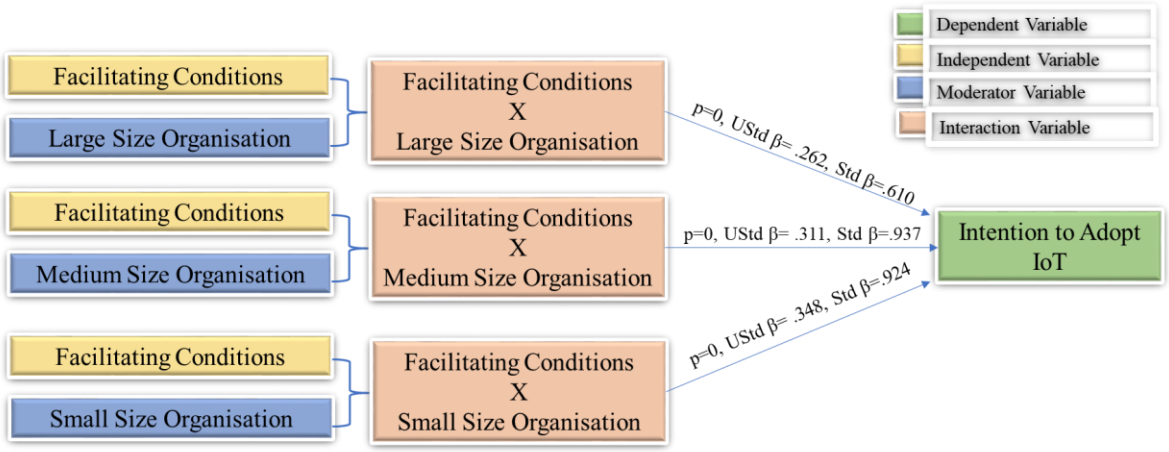

Figure 5-5: Model with interaction variable Facilitating Conditions and Organization Size

5.4 Comparison of finding of research with existing literature

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. Security issues will have a hindering effect on the adoption of the IoT (Roman, 2011). The second view decipher that users take security as granted. Some of the literature stated that users often trade privacy and security for convenience (Bojanova, 2014). 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 (Chevalier, 2021). 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 (Anand, 2020).

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 (Sair, 2018). However, there are literatures that contradict this through. For Facebook, the direct effect of the performance expectancy on user behaviour was not significant. Also, in the case of Twitter, performance expectance does not play a significant role (Pena, 2017). 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. In the previous researches about other technologies, the relationship proved to be positive and significant repeatedly while it's not a significant factor as per the outcome of study (Lee, 2018). The IoT landscape is highly interactive, ubiquitous, and self-sufficient 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 (Sair, 2018).

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 aspectto influence consumer intention to adopt IoT (Ambrawati, 2020). Almost all research papers and studies revealed that it's one of the most important constructs in adoption of technologies (Lu, 2005).

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.

5.5 Implications for service providers

As IoT service providers assume security as the main factor hindering the adoption of IoT in the manufacturing industry, this research is giving them details of other factors and their impact. The IoT service provider can use this research to focus on the right area to improve the adoption of IoT and increase their customer base to enhance profitability. As per research, performance expectancy, effort expectancy and facilitating conditions plays significant role along with security awareness in consumer intention to adopt IoT. Further, these factors are applicable in all size of the organisations. These factors strongly applicable for medium and small size organisations whereas moderately applicable in large size organisations. Hence, service provides can build solutions keeping medium and small size organisation requirements in mind and give them low budget solutions. Changing their marketing strategy for medium and small scale organizations can also improve the adoption.

5.6 Implications for Government, Regulatory bodies, and Policy makers

As government initiatives through Industry 4.0 showed a positive impact on automation in the manufacturing sector, the government should continue creating awareness about the benefits of automation through IoT. Relaxation in taxes could be another initiative to extend the acceptance of IoT. Also, the central government and state government should work on better and safe infrastructure to enhance the acceptance of IoT.

The study may be helpful to regulatory bodies and policymakers to create confidence in customers regarding IoT. With this study regulatory bodies can identify factors that play an important role in the adoption of IoT. The governments can introduce loan on low interest for the deployment of IoT in manufacturing organizations.

5.7 Implications for Academic Institution

The study can also help the institutions to design courses related to IoT technology. The special course can be added to the curriculum for imparting literacy on IoT usage, installation, troubleshooting and security. It will help institutions to increase students as well as the industry by providing a skilled force.

5.8 Implications for Researchers

The findings of this research bring out the significance of various factors that impact the adoption of IoT which were not tested before. Three factors of TAM Model along with security awareness could

be used in other research models to include various other factors that have not been tested or evaluated before. As this research is made on manufacturing industry in Mumbai and surrounding areas, same can be extended to other regions.

5.9 Limitations of the research

This study, factors affecting adoption of internet of things in India industry: A study in manufacturing company in and around Mumbai has been performed to explore the reasons which impact the adoption of IoT. 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) along with Security Awareness. The four factors studied are performance expectancy, effort expectancy, facilitating conditions and security awareness. The influence of organisation size on these factors are also studied. These factors are very important factors 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.

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 city might give different results.

5.10 Suggestion for future research

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 that will enhance users' understanding on latest security threats and impact which can change the viewpoint of users over time.

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.

This research is performed on manufacturing companies. The model created from this research can be extended to other industries to take benefit.

5.11 Concluding Remarks

The research is a sincere attempt to identify the factors that influence consumers' intention to adopt IoT in manufacturing organizations. Three factors are taken from the TAM model that is the most accepted model for technology adoption. Security awareness is added as a factor that is studied by the different researchers as an independent factor. Subsequently, the research is extended to the size of the organization. The research concludes that three factors of the TAM model, performance expectancy, effort expectancy, and facilitating conditions along with security awareness influence the consumer intention to adopt IoT in manufacturing organizations. The extended study on the size of the organization gives a piece of very useful information that medium and small size organisations strongly moderates above factors in adoption of IoT while moderation is low from large scale organizations. This conclusion of the research gives valuable information to the IoT

service providers, government, and industry policymakers to give focus on the medium and small segment industries to improve IoT adoption to take its benefits.

BIBLIOGRAPHY

BIBLIOGRAPHY

Books

1. Donald, R. C., Pamela S. S. & J. K. S., Business Research Method (11th Edition) (2015), McGraw Hill Education.

2. Bahga, A & Madisetti, V., Internet of Things: A hands-on Approach (2015), Universities Press India Pvt. Ltd.

3. 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.

4. 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.

5. 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).

6. 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.

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

8. Galero, T.E. (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.

9. Pallant, J. (2005). SPSS survival manual: a step by step guide to data analysis using SPSS. Allen & Unwin Publication

10. Ruggieri, M. & Nikookar, H. (2014). Internet of things- From research and Innovation to Market Development. River Publication.

Journal Articles

1. 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

2. Basset, M.A., Manogaran, G. & Mohamed, 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.

3. Xi-Jun, L. H. (2015). 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

4. Luigi Atzori, A. I. (2010). The Internet of Things: A Survey. Elsevier, 1-19. Retrieved from https://www.cs.mun.ca: https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf

5. Chao, C. M. (2019). 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

6. Roman R, Nagera, P. & Jopez, J. (2011). Securing the Internet of Things. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/220475753_Securing_the_Internet_of_Things

7. Bojanova, I., Hurlburt, G., & Voas, J. (2014). Imagineering an Internet of Anything. Retrieved from https://ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/6838944

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

9. Almaiah, M. A. (2019). 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

10. Shah, S. K. A. & Mahmood, W. (2020). 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

11. Nystroma, P.C., Ramamurthy, K. & Wilson, A. L. (2002). Organizational context, climate and innovativeness: adoption of imaging technology. Retrieved from Sciencedirect.com: https://doi.org/10.1016/S0923-4748(02)00019-X

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

13. Jones, N. B. & Graham, C. M. (2020). Can the IoT helps small business? Retrieved from Research gate: 10.1177/0270467620902365

14. Dizon, E. & Paranggno, B. (2021). 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

15. Khan F., Siddique, M. A. B., Rehman, A. U. & Jadoon, J. K. (2020). IoT Based Power Monitoring System for Smart Grid Applications. Retrieved from Researchgate.com: 10.1109/ICEET48479.2020.9048229

16. Dagar, R., Som, S. & Khatri, S. (2018). Smart Farminig In IoT infrastructure. Retrieved from IEEE: 10.1109/ICIRCA.2018.8597264

17. Sitenkov, D. (2014). Access Control in the Internet. Swedish ICT-SICS. Retrived from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1043405&dswid=8138

18. Roshan R. & Ray, A. K. (2016). Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective. International Journal of Computer Applications, Volume 153 – No3.

19. Kowatsch, T. & Maass, W. (2012). Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts

20. Kruger, H. A. & Kearney, W.D. (2006). A prototype for assessing information security. computers & s e c u rity , 2 8 9 – 2 9 6.

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

22. Bertini, M. M. (2016). The Impact of Technology Acceptance and Openness to Innovation on Software. ProQuest.

23. Venkatesh, V., Thongt, J. Y. L. & Xing X. (2013). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. Association of Information Security.

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

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

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

27. Venkatesh, V., Thongt, J. Y. L. & Xing X. (2012) . Consumer Acceptance and Use of Information. MIS Quarterly, 157-178.

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

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

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

31. 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.

32. Hull, G., John, H. & Budi, A. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Springer.

33. Alaba, F.A., Othman, M., Abaker, I., Hashem T. & Alotaibi, F. (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

34. Delipi, F. & Yayilgan, S. Y. (2016). Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. Retrived from https://ieeexplore.ieee.org/document/7592702.

35. Babar, S., Stango, A., Prasad, N., Sen, J. & Prasad, R. (2011). Proposed Embedded Security Framework for Internet of Things (IoT). https://ieeexplore.ieee.org/document/5940923.

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

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

38. Friedewald, M. & Raabe, O. (2011). Ubiquitous computing: An overview of technology impacts. Science Direct, 55-65.

39. Baldini, G., Botterman, M., Neisse, R. & Tallacchini, M. (2018). Ethical Design in the Internet of Things. Springer, 905-925.

40. 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

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

42. 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

43. Marathe, A. (2018). Internet of Things: Opportunities and applications in pharmaceutical manufacturing and logistics. Retrived from https://www.researchgate.net/publication/328269133_INTERNET_OF_THINGS_OPPORTUNITIES_AND_APPLICATIONS_IN_PHARMACEUTICAL_MANUFACTURING_AND_LOGISTICS.

44. Lind, M. R., Zmud, R.W. & Fischer, W. A. (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

45. Hittinger, E. & Jaramillio, P.(2019). Internet of Things: Energy boon or bane. ScienceMag, Vol. 364, Issue 6438, 326-328.

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

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

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

49. Tan, J.J. & Poslad, S. (2007). A Semantic Approach to Harmonizing Security Models for Open Services. Applied Artificial Intelligence, 353-379. Retrieved from https://doi.org/10.1080/08839510500484298

50. Lai, P. (2017). The Literature Review of Technology Adoption Models and Theories For The Novelty Technology. Journal of Information Systems and Technology Management, 21-38.

51. Venkatesh, V., Thong, J. Y. L. & Xu, X. (2012, March). Consumer Acceptance and Use of Information. MIS Quarterly, 157-178.

52. Alenezi, A., Zulkipli N. H. N., Atlam, H. F. & Wlters, R. J. (2017). The Impact of Cloud Forensic Readiness on Security, 511-517. Retrived from https://www.researchgate.net/publication/317299421_The_Impact_of_Cloud_Forensic_Readiness_on_Security

53. Patrick, S., Christa, B. & Lothar, S. (2018). Correlation Coefficients: Appropriate Use and Interpretation. Anesthesia & Analgesia, 1763-1768. Retrieved from https://journals.lww.com/anesthesia-analgesia/fulltext/2018/05000/correlation_coefficients__appropriate_use_and.50.aspx

54. Sair, S. A. & Danish, R. Q. (2018). Effect of Performance Expectancy and Effort Expectancy on the Mobile Commerce Adoption Intention through Personal Innovativeness among Pakistani Consumers. Research Gate, 501-520. Retrieved from https://www.researchgate.net/publication/327702133_Effect_of_Performance_Expectancy_and_Effort_Expectancy_on_the_Mobile_Commerce_Adoption_Intention_through_Personal_Innovativeness_among_Pakistani_Consumers

55. Ambrawati, R., Dian, H. Y. & Suyono, T. (2020). The Role of Facilitating Conditions and User Habits: A Case of Indonesian Online Learning Platform. The Journal of Asian Finance, Economics and Business, 481-489.

56. Lu, J., Yu, C.S. & Liu, C. (2005). Facilitating Conditions, Wireless Trust and adoption intention. Journal of Computer Information, 17-24.

57. Oh S. & Letho, X. Y. (2009). Travelers' Intent to Use Mobile Technologies as a Function of Effort and Performance Expectancy. Journal of Hospitality Marketing & Management , 765-781.

58. Fisher, R. A. (1915). Frequency Distribution of the Values of the Correlation Coefficient in Samples from an Indefinitely Large Population. Biometrika, 507-521.

59. Atzori, L., Lera, A. & Morabito, G. (2010, May). The Internet of Things: A Survey. Elsevier, 1-19. Retrieved from https://www.cs.mun.ca: https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf

60. 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.

61. Keong, M. L., Ramayah, T., Kurnia, S., & Chiun, L. M. (2012). Explaining intention to use an enterprise resource planning (ERP) system: an extension of the UTAUT model. Business Strategy Series, 13(4), 173 - 180. doi: 10.1108/17515631211246249.

Conferences

1. Wylde, G., Costa, C. D. & Ellen P. (2020). Accelerating the Impact of Industrial IoT in small and medium size business. World Econimic Forum. Geveva, Switzerland: World Economic Forum.

2. Medvedev, A., Zaslavsky, F. A., Anagnostopoulos, T., Khoruzhnikov, S. (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.

3. Marques, G. & Pitrama. R. (2019). Noise Monitoring for Enhanced Living Environments Based on Internet of Things. World Conference on Information System and Technology (pp. 45-54). Springer.

4. 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.

Web Sites

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

2. Evans, D. (2011, April). http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Retrieved April 2017, from http://www.cisco.com.

3. Dinesh Malkani. (2015). http://www.cisco.com/c/en_in/about/thought-leadership/reaching-infection.html. Retrieved April 2017, from http://www.cisco.com: http://www.cisco.com

4. Intuit Technology Services Private Limited. Understanding and Overcoming Barriers to Technology Adoption Among India's Micro, Small and Medium Enterprises. Retrieved from www.intuit.in: www.intuit.in/images/MSME%20White%20Paper_FINAL.pdf

5. Testing for Normality using SPSS Statistics. (2018). (Lund Research Ltd) Retrieved from https://statistics.laerd.com/spss-tutorials/testing-for-normality-using-spss-statistics.php

6. Skewness-Kurtosis All Normality Test. Retrieved from https://variation.com/wp-content/distribution_analyzer_help/hs133.htm#:~:text=The%20Skewness%2DKurtosis%20All%20test,zero%20and%20kurtosis%20of%20three.

7. Anaesth, A. C. (2019). Descriptive Statistics and Normality Tests for Statistical Data. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6350423/

8. 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

9. 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/

10. Brumfitt, H. A., Askwith, R. & Zhou, B. (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

11. 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/

12. 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

13. 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

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

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

16. 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

17. 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

18. 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

19. 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/

20. 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

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

22. 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

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

24. 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/

25. 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

26. 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

27. Khan, W. Z. & Khan, M. K. (2019). 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

28. IOWA, C. I. What is confidential data? Retrieved from https://iso.iowa.gov: https://iso.iowa.gov/faq/what-confidential-data

29. 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

30. Saputo, P. Electronic Data Tampering. Retrieved from https://saputo.law: https://saputo.law/criminal-law/texas/electronic-data-tampering/

31. Swinhoe, D. (2019). 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

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

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

34. 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

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

36. Hernández-Ramos, J. L., Bernabe, J. B., Moreno, M. V. & Skarmeta, A. F.(2015). 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

37. Wray, S. (2016). 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/

38. Mykola, O. (2020). 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/

39. 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

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

41. Sarin, A. (2018). 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

42. D'mello, A. (2020). 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/

43. Singh, A. (2019). 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

44. All, I. F. (2019). https://www.iotforall.com. Retrieved from 7 Challenges of IoT Software Development: https://www.iotforall.com/iot-software-development-challenges

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

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

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

48. Wiessberger, A. (2020). 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.

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

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

51. IDC. (2019). IDC. Retrieved from https://www.idc.com: https://www.idc.com/getdoc.jsp?containerId=prUS45612419

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

53. Hanan Aldowah, S. U. (2019). 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. Formplus. (2004). Formplus. Retrieved from https://www.formpl.us: https://www.formpl.us/blog/correlational-research

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

56. 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/

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

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

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

60. 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/

61. Frost, J. (2021). Statistics By Jim. Retrieved from https://statisticsbyjim.com: https://statisticsbyjim.com/glossary/standard-error-regression/

62. 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

63. Kassner, M. (2020). 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/

64. Bednarz, A. (2018). 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

65. Arampatzis, A. (2019). 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

66. Chao, C.-M. (2019). 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

67. Micro, T. (2020). 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

68. Al-Qeisi, K. I. (2009). Analyzing the Use of UTAUT Model in Explaining an Online. Retrieved from https://core.ac.uk: https://core.ac.uk/download/pdf/40049467.pdf

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

70. Yogesh K. Dwivedi, N. P. (2017). 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

71. Grizhnevich, A. (2018). 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

72. Zhao, Y. L., (2020). 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

73. Ganti, A. (2021). Central Limit Theorem (CLT). Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/c/central_limit_theorem.asp#:~:text=Key%20Takeaways-,The%20central%20limit%20theorem%20(CLT)%20states%20that%20the%20distribution%20of,the%20sample%20size%20gets%20larger.&text=A%20key%20aspect%20of%20CLT,population%20me

74. 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/

75. Anand, S. (2020). 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

76. Pena, J. & López, M. (2017). 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

77. Lee, W. (2018). 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

78. Pal, D., Funilkul, S., Charoenkitkarn, N. & Prasert, K. (2018). 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

79. 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

80. 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

81. Lee, J. & Baek, S. I.(2011). 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

82. Morley, H. R. (2018). 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

83. 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

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

85. Howard, D. M. (1951). Introduction to Cronbach's Alpha. Retrieved from https://mattchoward.com: https://mattchoward.com/introduction-to-cronbachs-alpha/

86. Solutions, S. (2021). Quantitative Research Approach. Retrieved from https://www.statisticssolutions.com: https://www.statisticssolutions.com/quantitative-research-approach

87. Jaadi, Z. (2019). Everything you need to know about interpreting correlations. Retrieved from https://towardsdatascience.com/eveything-you-need-to-know-about-interpreting-correlations-2c485841c0b8

88. Editor, M. T. (2013). Regression Analysis: How Do I Interpret R-squared and Assess the Goodness-of-Fit? Retrieved from https://blog.minitab.com: https://blog.minitab.com/en/adventures-in-statistics-2/regression-analysis-how-do-i-interpret-r-squared-and-assess-the-goodness-of-fit

89. 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/

90. Frost, J. (2021). Statistics By Jim. Retrieved from https://statisticsbyjim.com: https://statisticsbyjim.com/glossary/standard-error-regression/

91. Potters, C. (2021). R-Squared vs. Adjusted R-Squared: What's the Difference? Retrieved from Investopedia: https://www.investopedia.com/ask/answers/012615/whats-difference-between-rsquared-and-adjusted-rsquared.asp

92. UCLA. (2021). Statical Consulting. Retrieved from https://stats.idre.ucla.edu: https://stats.idre.ucla.edu/spss/faq/coding-systems-for-categorical-variables-in-regression-analysis-2

93. Chevalier, M. (2021). Security. Retrieved from https://www.securitymagazine.com: https://www.securitymagazine.com/articles/89202-small-and-mid-size-businesses-need-to-focus-on-cybersecurity

Thesis

1. Nyandoro, C. K. (2016). Factor influencing information communication technology acceptance and use in small and medium enterprises in Kenya. Pro Quest, January. Retrived from https://www.proquest.com/openview/4a08e40ce4e0c17c7791e7d9c07661b4/1?pq-origsite=gscholar&cbl=18750#:~:text=This%20study%20evaluated%20factors%20of,influential%20factors%20of%20ICT%20acceptance.

2. Harper, A. A. (2016). 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.

3. Phuoc, H. M. P. (2019). Impact of IoT Technology on Digital Servitization and Business Performance of Manufacturing Firms. Retrieved from https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=toledo1566550331986294&disposition=inline

4. Anastasia, V. (2018). Determinants of User Adoption of eGovernment Services: The Case of Greek Local Government. Retrieved from https://eprints.mdx.ac.uk/25869/1/AVoutinioti%20thesis.pdf.

APPENDICES

Appendix A: QUESTIONNAIRE

Dear Sir/Madam,

I am a doctoral candidate from ICFAI. I am currently collecting data for my research on - ***Factor Affecting Adoption of IoT in Indian Industry: A Study in Manufacturing Companies in and Around Mumbai.*** *Your participation in survey would help me in this research. The information provided by you will be used for academic purpose only. The participation in survey is volunteer and there is no right or wrong answer.*

What is IoT (Internet of Things)

The Internet of Things refers to the networking of physical objects with unique identifier and embedded with sensors. These devices can collect information from other devices and/or transmit information about the devices without human-to-human or human-to-computer interaction. The data collected from these devices can then be structured, analysed to optimize products, services, and operations through automation.

Today, data resides everywhere in an enterprise—Resource Planning (ERP) system, Product Lifecycle Management (PLM) systems, Manufacturing Execution Systems (MES) and Supplier Relationship Management (SRM) systems, in machine tools and in thousands of spreadsheets, files and folders across the company. Data also resides outside the enterprise, across the value chain with partners on both the supply and the sales sides. The goal of Internet of thing is to break down organizational processes, data and system silos and automate the collection of data across operations using embedded sensors. The collected data is deeply analysed for systems and machines to take decisions without human intervention. An enterprise that uses a deeper, wider and smarter analysis of its data will see big operational dividends.

Name		***Organization Name***	
Email		***Organization Address***	
Contact No		***Industry like Electronics, IT , Telecom, Chemical***	
Your Age Group		***Other Industry***	
Designation		***Number of Employees***	
Qualification		***Turnover in INR*** *(Approximate)*	
Experience in Years			

1	*I am aware of IOT*							
2	*If Yes, Source of Information*	News Paper, magazines	Internet	*Webinar*	*Seminars*	*Experienced IoT usage in same or different Industry*	*Other*	
3	*I am using IoT for my business.*							
4	*If yes, Mentions its application (Which area IoT is implemented)*							
5	*If No, Am I willing to use IOT for my business*							
6	*If you are not willing, Please give reason*							
			Strongly Agree	Agree	Neutral (Neither Agree nor Disagree)	Disagree	Strongly Disagree	
	Intention of using IoT							
7	If I had access to IoT , I would have the intention of using it.							
8	I will always try to use IoT for my business.							
9	I think it will be worth it for me to adopt IoT when it's available.							
10	Assuming I have access to use IoT for my business, I would use it							
11	Given opportunity, resources and knowledge, I would use IoT for my business							
	Security Awareness							
12	I have threat to loose business data by using IoT.							
13	I have threat from hackers who can access systems and impact business.							
14	The business confidential information is not safe using IoT							
15	The chances of virus and malware attack increase with use of IoT							
16	The privacy is compromised using IoT							

Performance Expectancy								
17	Using IoT in my job would enable me to accomplish task more quickly							
18	Using IoT would make it easy to do my job							
19	IoT improves the quality of work I do							
20	Using IoT would increase my productivity							
21	Use of IoT can decrease the time to do the important jobs							
22	Use of IoT can improve the quality of output significantly							
Effort Expectancy								
23	Learning how to use IoT for my business is easy for me.							
24	My interaction with IoT is clear and understandable.							
25	I find IoT easy to use.							
26	It is easy for me to become skilful at using IoT.							
Facilitating Conditions								
27	I have the resources necessary to use IoT for my business							
28	I have the knowledge necessary to use IoT for my business.							
29	The IoT systems are compatible with other technologies I use.							
30	I can get help from specialist people or group when I have difficulties using IoT							

Appendix B: PUBLICATIONS AND PRESENTATIONS BY SCHOLAR IN THE RESEARCH AREA

Papers Published

1. A paper titled “Factors Impacting Adoption of IIoT” published in Turkish online journal of qualitative inquiry volume 12, No 6, (2021) ((ISSN: 1309-6591) (Gurvinder Singh, Dr.Tarak Nath Paul, Dr. Sushil Kumar Pare).
2. A paper “Impact of Security Awareness on Adoption of Industrial Internet of Things” published in Solid State technology Vol. 63 No. 6 (2020) page no 11(ISSN: 0038-111X) (Gurvinder Singh, Dr.Tarak Nath Paul, Dr. Sushil Kumar Pare).
3. A paper “The Internet of Things (IoT) - Imperative for Our Survival” published in ICFAI, Jharkhand Journal on IoTof October 2016 (Gurvinder Singh).
4. A paper “Project Management in Dynamic Environment” published in ICFAI, Jharkhand journal through Doctoral Conference on Trends in Management Research held on 9th March 2017 at Jharkhand (Gurvinder Singh).

Conferences Attended

1. International Conference on IoT in Social, Industry, Analytics and Communication (IoT-SIAC 2020) held on November 27th & 28th, 2020 at Thakur College of Engineering and Technology, Kandivali (E), Mumbai.
2. National Conference on Business Dynamics: Local to Global held on February 5th and 6th, 2021 at D Y Patil Institute of Management Study at Navi Mumbai.