Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 6, July 2021: 5202-5207

FACTORS IMPACT ADOPTION OF INDUSTRIAL INTERNET OF THINGS

Gurvinder Singh[1], Dr. Tarak Nath Paul[2], Dr. Sushil Kumar Pare [3]

[1]PhD Scholar, ICFAI University, Jharkhand, Ranchi, India
gurvinder30@gmail.com
[2]Assistant Professor, ICFAI University Jharkhand, Ranchi
paultarak@gmail.com
[3]Associate Professor, Thakur Institute of Management Studies & Research, Mumbai
dr.pare@gmail.com

ABSTRACT:
The manufacturing industries are under tremendous pressure to improve production quality, increase production efficiency, stay competitive, enhance employee safety, data security and remain profitable. The IIoT is the only hope which can support manufacturing organisations to stay competitive. There are multifold advantages from IIoT for manufacturing industries. This paper investigates four factors which can impact adoption of IIoT in manufacturing industries. These four factors are Awareness of security threats, Performance Expectancy, Effort Expectancy and Facilitating Conditions. There are many papers and articles highlight that awareness of security threats are main concern in adoption of IIoT. This paper will explore if other reasons are impacting adoption of IIoT or not.

I. NTRODUCTION

The Internet of Thing (IoT) has been firstly defined as a system of interconnected devices [1]. IoT named devices with smart interferences and identity that can connect and communicate to add value to their environment and users [2]. The scope of IoT application 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, application of IoT in industrial and manufacturing segments is known as Industrial Internet of Things (IIoT). The IIoT has revolutionized factory and industrial segmentations through its excellence which is outcome of automation. Far greater efficiency, accuracy, scalability, money saving, time saving, predictive maintenance and many other values are instances of IIoT benefits [3]. However, this emerging phenomenal (IIoT) has its own concerns for adaption. According to Gartner forecast, information security is a top concern among enterprises adapting IoT [4]. Security concerns are 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 at most should be considered of the impact of security threats and cyber-attacks in IIoT. Studying IoT security threats in different application specifically in industrial segmentation is an ongoing research area in academic and industrial surveys. There are other factors which are equally important to be considered and have major impact on adoption of IIoT. However, every limited article, research papers have explored it. As per Unified Theory of Acceptance and Use of Technology (UTAUT) by Viswanath Venkatesh, there are four factors which playing significant role in adoption of technologies and these factors are Performance Expectancy, Effort Expectancy, Facilitating Conditions and Social Influence. This paper will explore if Awareness of Security threat impacts the adoption of IIoT or Performance Expectancy, Effort Expectancy, Facilitating Conditions also plays a role in decision of IIoT adoption. Before analysis, its important to understand the definition of each team.

A. **Performance Expectancy:** Performance expectancy is defined as the consumers' expectation that use of IoT will improve in the performance. Performance expectancy is drawn from other constructs, including perceived usefulness of the TAM [5]. Performance expectancy was found to be the strongest predictor of behavioral intention to use technology [6].

B. **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 [5].

C. **Facalitating Conditions:** Facilitating conditions are defined as a collection of perceived infrastructure 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 .

II. PROBLEM DEFINITION

There are many research literatures on the IoT which addressed that there are substantial security issues with IoT which are unresolved. "Although the technology of the IoT has great potential, security issues continue to plague the technology" [7]. The user data privacy and security are major concern. In the area of wireless, data transfer integrity is at risk. Several authors pointed out that 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" [8]. However, it is still not qualified that awareness of security threats is the primary reason in acceptance of IoT or there are other drivers which are contributing in decision making of adoption of IoT.

III. SOLUTION

This study is conducted to understand how Security Awareness, Performance Expectancy, Effort Expectancy and Facilitating Conditions impact adoption of IIoT among entrepreneurs and senior staff of manufacturing industry in and around Mumbai. The report will help IIoT vendors, service providers, and business managers to understand if awareness of security threats is the sole barrier in adoption of IIoT in large, medium and small manufacturing enterprises in and around Mumbai or other three factors are also playing role in decision making in adoption of IIoT. It will help them work on removing those barriers.

The study is conducted on 50 manufacturing companies form different areas like Pharmaceutical, Petroleum, Textile, Chemicals, Electronics etc. The data is collected through face to face and telephonic interviews.

VI. DATA COLLECTION AND ANALYSIS

A survey was conducted, and data is collected form 50 entrepreneurs and senior staff of manufacturing complies in and around Mumbai. The survey was designed to answer different questions to understand their awareness on security threats, facilitating conditions, performance expectancy, effort expectancy of IIoT.

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

- Normality test for dependent variable through Skewness & Kurtosis test.
- Reliability test of independent variable using Cronbach's alpha.
- Multicollinearity test for each independent variable through Variance Inflation (VIF)
- Remove outliers from data with Standardized residual value greater than 2
- Multiple regression test of all independent variable with dependent variable.

Adoption of IIoT is a dependent variable which is evaluated through a question to check if IIoT is adopted by an enterprise or not. The independent variables are security threats awareness, performance expectancy, effort expectancy and facilitating conditions which are checked through different questions in survey.

A. **Normality Test of Dependent Variable:** The normality test of data is a qualification for many statistical tests because normal data is a fundamental assumption in testing. The normality can be tested graphically and numerically. Graphical interpretation has the advantage of allowing good judgement to assess normality in situations when numerical tests might be over or under sensitive, but graphical methods do lack objectivity. "If you do not have a great deal of experience interpreting normality graphically, it is probably best to rely on the numerical methods" [9]. There are different methods to test data normality. The Skewness & Kurtosis and Smirnov and Shapiro are most accepted tests for normality and used in this research.

1) *Skewness & Kurtosis Test.* "It is one of the most used test for normality among three general normality tests (Anderson-Darling Test, Shapiro-Wilks Test, Skewness-Kurtosis) designed to detect all departures from normality. It is comparable in power to the other two tests" [10]. If normality test fails, it allows you to state with 95% confidence the data does not fit the normal distribution. On passing the normality test, allows you to state no significant departure from normality was found.

If skewness = 0, the data are perfectly symmetrical. But a skewness of exactly zero is quite unlikely for real-world data, so how can you interpret the skewness number? The suggested rule of thumb is:

- If skewness is less than −1 or greater than +1, the distribution is highly skewed.
- If skewness is between −1 and −½ or between +½ and +1, the distribution is moderately skewed.
- If skewness is between −½ and +½, the distribution is approximately symmetric [11].

The test result of Skewness test in Table I is -.421 (SE .337) which is between −½ and +½ and proves that data is approximately symmetric.

The Kurtosis test result is -1.90 (SE .662) in Table I which proves it is light tailed distribution [12].

B. Reliability Test of independent variables: Cronbach's alpha test measures internal consistency. It provides information that how closely items in a group are related. It is considered to be a measure of scale reliability. It is used under the assumption that you have multiple items measuring the same underlying construct. "The general rule of thumb is that a Cronbach's alpha of .70 and above is good, .80 and above is better, and .90 and above is best" [13]. The Cronbach Alpha test is used here to check reliability of independent variables which are Security Treats Awareness, Performance Expectancy, Effort Expectancy and Facilitating Conditions.

TABLE I. SKEWNESS & KURTOSIS TEST

			Statistic	Std. Error
I am using IoT for my Business	Mean		1.6	0.07
	95% Confidence Interval for Mean	Lower Bound	1.46	
		Upper Bound	1.74	
	5% Trimmed Mean		1.61	
	Median		2	
	Variance		0.245	
	Std. Deviation		0.495	
	Minimum		1	
	Maximum		2	
	Range		1	
	Interquartile Range		1	
	Skewness		**-0.421**	**0.337**
	Kurtosis		**-1.9**	**0.662**

TABLE II. SECURITY THREATS AWARENESS RELIABILITY STATISTICS

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

TABLE III. PERFORMACE EXPECTANCY RELIABILITY STATISTICS

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

TABLE IV. EFFORT EXPECTANCY RELIABILITY STATISTICS

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

TABLE V. FACALITATING CONDITION RELIABILITY STATISTICS

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

	Items	
0.947	0.945	5

The Table II shows Cronbach Alpha test for Security Threat Awareness, Table III shows it for Performance Expectancy, Table IV depicts results of Effort Expectancy and Table V shows results of Facilitating Conditions. All these results are greater than .9 which concludes reliability of four independent variables.

C. Multicollinearity Test for Independent Variables: The "Multicollinearity occurs when independent variables in a regression model are correlated. This correlation is a problem because independent variables should be independent. If the degree of correlation between variables is high enough, it can cause problems when you fit the model and interpret the results" [14]. "Statistical software calculates a VIF for each independent variable. VIFs start at 1 and have no upper limit. A value of 1 indicates that there is no correlation between this independent variable and any others. VIFs between 1 and 5 suggest that there is a moderate correlation, but it is not severe enough to warrant corrective measures. VIFs greater than 5 represent critical levels of multicollinearity where the coefficients are poorly estimated, and the p-values are questionable" [14]. The tables VI, VII, VIII, IX and X are depicting multicollinearity test of four independent variables and VIF values for all the tests is 1 which concludes that there is no correlation among 4 independent variables.

TABLE VI. SECURITY AWARENESS Vs PERFORNACE EXPECTANCY

Model	Collinearity Statistics	
	Tolerance	VIF
Performance Expectancy	1.000	1.000

TABLE VII. SECURITY AWARENESS Vs EFFORT EXPECTANCY

Model	Collinearity Statistics	
	Tolerance	VIF
Effort Expectancy	1.000	1.000

TABLE VIII. SECURITY AWARENESS Vs FACILITATING CONDITION

Model	Collinearity Statistics	
	Tolerance	VIF
Facilitating Condition	1.000	1.000

TABLE IX. PERFORNACE EXPECTANCY Vs FACILITATING CONDITION

Model	Collinearity Statistics	
	Tolerance	VIF
Facilitating Condition	1.000	1.000

TABLE X. EFFORT EXPECTANCY Vs FACILITATING CONDITION

Model	Collinearity Statistics	
	Tolerance	VIF
Facilitating Condition	1.000	1.000

D. Standardized Residual and Data Outliers: Standardized Residual is conducted on dependent and independent variables to remove data which is out of range. In this research, the values of different questions asked in dependent and independent variables are averaged out to get one value. Thereafter, standard residual was run using SPSS software. In fig. 1 lowest value is -1.5 and highest is +2.5. Any value which is outside this range is outliered. The data in 50th row is outside the range and removed.

E. Multiple Regression: "Multiple regression is an extension of simple linear regression. It is used when we want to predict the value of a variable based on the value of two or more other variables. The variable we want to predict is called the dependent variable. The variables we are using to predict the value of the dependent variable are called the independent variables" [15].A low p-value (< 0.05) indicates an independent variable is likely to impact dependent variable. Conversely, a larger p-value (>0.05) suggests that changes in the dependent variable are not associated with changes in the independent variable. In this research, to know the impact of four independent variables Security Awareness, Performance Expectancy, Effort Expectancy and Facilitating Conditions on adoption of IIoT which is a dependent variable, multiple regression was conducted with following results.

TABLE XI. MULTIPLE REGRESSION

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.861	0.268		3.216	0.002
	Security Awareness	-0.06	0.054	-0.111	-1.101	0.277
	Performance Expectancy	0.114	0.075	0.182	1.52	0.136
	Effort Expectancy	-0.007	0.059	-0.015	-0.117	0.907
	Facilitating Condition	0.285	0.065	0.638	4.365	0

The Table XI shows p-value of four independent variables which concludes that Security Awareness, Performance Expectancy, Effort Expectancy independent variables do not have much impact on dependent variable. However, independent variable Facilitating Condition is corelated with dependent variable adoption of IIoT. The change in Facilitating condition will change adoption of IIoT.

VII. CONCLUTION

Most of the articles on IoT explains security as one of the main bottlenecks in adoption of IoT. The data theft, virus, malware attacks, privacy issues are the main concerns in slow adoption of IoT.

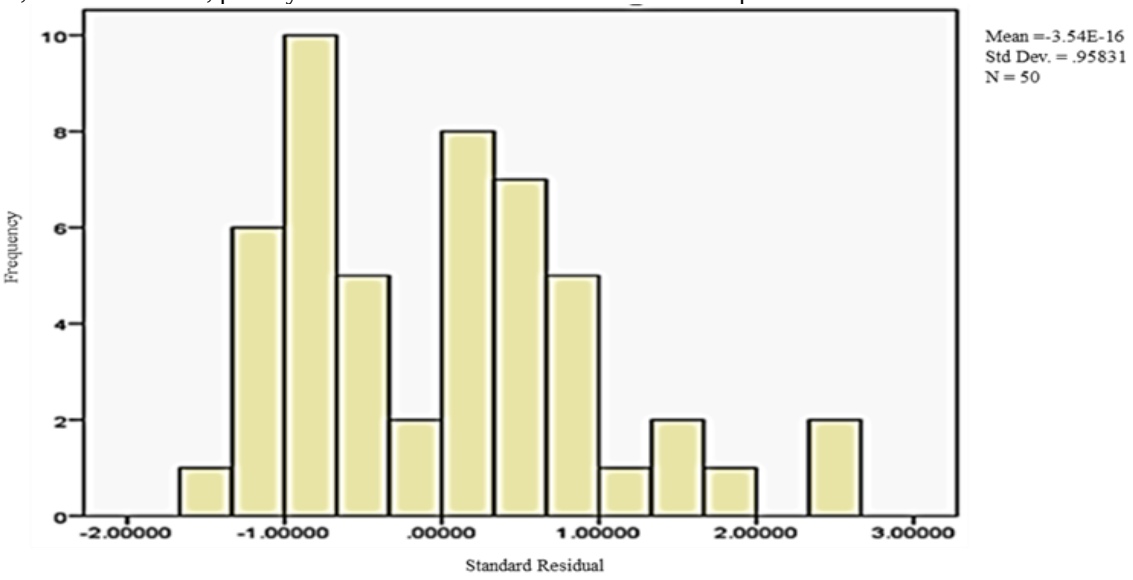

Fig 1. Standard Residual

When we talk about IoT adoption in manufacturing industries there are several cyber security threats highlighted like phishing attacks, malware attacks, DDoS attack etc which is slowing its adoption. However, study on 50 participants who are from manufacturing industry in and around Mumbai gives different results. The industrialists, senior staff and IT staff of manufacturing organizations are aware of security concerns however they are prepared to deal with it and ready to take advantages of IIoT. The study reveals that there are other

factors which are responsible for decelerating adoption of IIoT and Facilitating Conditions is the main concern. There is requirement to build appropriate infrastructure which will enhance adoption of IIoT.

This study is conducted on manufacturing industries in and around Mumbai where many security service providers are available. The results of this study can differ for small and remote cities and can be an area for future studies. Similarly, the results can be varied for the non-manufacturing industries like health care, hospitality, banking and finance etc which can be explored in future studs.

REFERENCES

[1] M. W. A. K. a. S. M. M. Farooq, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, pp. 1-6, 2015.

[2] E. A. I. A. T. H. A. I. A. A. A. G. M. I. a. M. G. I. Yaqoob, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," IEEE Wireless Communications, pp. 10-16, 2017.

[3] Z. C. X. D. a. A. V. V. ". a. P. J. Zhou, Security and Privacy for Cloud-Based IoT, IEEE Communications Magazine, 2017.

[4] Gartner, "Forecast: IoT Security, Worldwide, 2016," 2016. [Online]. Available: https://www.gartner.com/en/documents/3277832/forecast-iot-security-worldwide-.

[5] D. Davis, "User Acceptance of information technology," Int. J Man- Machine Studies, pp. 475-487, 1993.

[6] J. Y. L. T. Viswanath Venkatesh, "CONSUMER ACCEPTANCE AND USE OF INFORMATION," MIS Quarterly , pp. 157-178, March 2012.

[7] L. H. Q. Xi-Jun, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," February 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404814001229?via%3Dihub.

[8] A. A. Harper, "The impact of consumer security awareness on adopting IoT," p. 16, 2016.

[9] "Testing for Normality using SPSS Statistics," Lund Research Ltd, 2018. [Online]. Available: https://statistics.laerd.com/spss-tutorials/testing-for-normality-using-spss-statistics.php.

[10] "Skewness-Kurtosis All Normality Test," [Online]. Available: https://variation.com/wp-content/distribution_analyzer_help/hs133.htm#:~:text=The%20Skewness%2DKurtosis%20All%20test,zero%20and%20kurtosis%20of%20three..

[11] M. G. Bulmer, "Principles of Statistics," in Principles of Statistics, 1979.

[12] "Engineering Statistics Handbook," 2012. [Online]. Available: https://www.itl.nist.gov/div898/handbook/eda/section3/eda35b.htm.

[13] "Cronbach's Alpha," 2019. [Online]. Available: https://www.statisticssolutions.com/cronbachs-alpha/.

[14] "Multicollinearity in Regression Analysis: Problems, Detection, and Solutions," 2019. [Online]. Available: https://statisticsbyjim.com/regression/multicollinearity-in-regression-analysis/.

[15] "Multiple Regression Analysis using SPSS Statistics," 2019. [Online]. Available: https://statistics.laerd.com/spss-tutorials/multiple-regression-using-spss-statistics.php.

[16] "testing-for-normality-using-spss-statistics," 2018. [Online]. Available: https://statistics.laerd.com/spss-tutorials/testing-for-normality-using-spss-statistics.php.

[17] A. C. Anaesth, "Descriptive Statistics and Normality Tests for Statistical Data," 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6350423/.