MEDIATING AND MODERATING FACTORS AFFECTING READINESS TO IOT APPLICATIONS: THE BANKING SECTOR CONTEXT

RashaAbd El-Aziz[1], Sarah El-Gamal[2] and Miran Ismail[1]

[1]Business Information Systems Department,College of Management and Technology, Arab Academy for Science, Technology and Maritime Transport, Miami Campus, Alexandria, Egypt
[2]Logistics and Supply Chain Management Department, College of International Transport and Logistics, Arab Academy for Science, Technology and Maritime Transport, AbouKir Campus, Alexandria, Egypt

ABSTRACT

Although IOT seems to be the upcoming trend, it is still in its infancy; especially in the banking industry. There is a clear gap in literature, as only few studies identify factors affecting readiness to IOT applications in banks in general, and almost negligible investigations on mediating and moderating factors. Accordingly, this research aims to investigate the main factors that affect employees' readiness to IOT applications, while highlighting the mediating and moderating factors in the Egyptian banking sector. The importance of Egypt stems from its high population and steady steps taken towards technology adoption. 479 valid questionnaires were distributed over HR employees in banks. Data collected was statistically analysed using Regression and SEM. Results showed a significant impact of 'Security', 'Networking', 'Software Development' and 'Regulations' on 'readiness to IOT applications. Thus, the readiness acceptance level is high'Security' and 'User Intention' were proven to mediate the relationship between research variables and readiness to IOT applications, and only a partial moderation role was proven for 'Efficiency'. The study contributes to increasing literature on IOT applications in general, and fills a gap on the Egyptian banking context in particular. Finally, it provides decision makers at banks with useful guidelines on how to optimally promote IOT applications among employees.

KEYWORDS

IOT applications; Readiness; IOT challenges; Banking sector; HRM practices; Structural Equation Modelling

1. INTRODUCTION

Information technology and digital economy have reshaped the business landscape around the world by changing the way organisations conduct business and the way services are delivered. Digitalization involves, but is not limited to, the digital transformation of business processes through the interaction of digital technologies such as mobile networks, cloud computing, artificial intelligence, and Internet of Things (IOT) with physical ICT infrastructure [12][48]. It also shows the influence of growing use of computers and communication channels [18] [83] [69]. Digitalization is the next industrial revolution and IOT is its core technology. IOT is a new paradigm promising a smart human being life by allowing communications between objects (things) such as televisions, lamps, cars, mobile phones or even plants connected by sensors through the Internet anywhere, anytime. IOT applications include Wristbands that act as an alarm

DOI: 10.5121/ijmit.2020.12401

and recognize sleeping patterns, Smartphones that can scan barcodes on food packages to provide information about its ingredients, and the gym that has a variety of applications enabling gathering information about the calories or body fat content [58]. Accordingly, IOT is expected to play an important role in many business areas [70] [23].

Despite the emergence of IoT applications, organisations face great challenges keeping up with an acceptable transformation pace, and achieving the expected results. Research on IOT has been recognized [45]by academics, and has gained banks' attention; especially in developing countries [46]. Yet, most of the studies were conducted on IOT adoption in general, with only few tackling factors that affect readiness to IOT applications in banks, negligible investigations on mediating and moderating factors, and almost none in the Egyptian context. The Egyptian banking industry in particular is one of the oldest and most critical in the region; especially due to its high population and steady steps it takes towards technology adoption [54]. Accordingly, the study at hand aims to present a thorough investigation of readiness to IOT applications in the banking industry, while highlighting the mediating and moderating factors. In order to achieve the research aim, the study seeks to answer the research questions: (1)What are the key factors affecting readiness to IOT applications in the banking sector? (2) What are the mediating and moderating factors affecting readiness to IOT applications in the banking sector?

This paper is structured into five sections: the first Section introduces the research and the study background, Section 2, provides a review of literature, Section 3, demonstrates the research framework and hypotheses, Section 4 illustrates the data collection and analysis. Section 5 draws conclusions, theoretical and practical implications, and provides suggestions for future work.

2. LITERATURE REVIEW

The digital economy has been identified as a wide network of economic and social activities, supported by digital technologies with an enormous potential to affect any organisation. Digitalization has been the upcoming trend; as it is the ability to turn existing products or services into digital variants, and thus offer advantages over tangible product [37][24][62] cited by[35].

In the last decade, IOT has played a significant role in the business landscape, making it fast moving and more competitive. Its great potential to enhance sustainability; which in turn optimizes operations and services [14], makes it an important topic to investigate.IOT is a network connectivity and computing capability that extends to objects, sensors and everyday items. Internet services have created new sets of data that include social networks data, pictures, videos, and a lot of textual information. But the real explosion of data variety is happening with the establishment and massive development of IOT [65] and [34]. Data generated from various domains helps to create valuable insights for optimizing operations and quality standards [6]. IOT is considered a wide-ranging network of smart 'things', associated with programs, electronics, hardware and network connectivity that empowers these things to accumulate and exchange data [17]. According to the Internet Architecture Board, IOT is a technology with a large number of embedded devices that employ Internet Protocols Communication Services and are not directly controlled by people [28]. It is a computing concept that describes a future where everyday objects are Internet-connected such as wearable devices or other sensor technologies [4].In 2017, IOT was reported as a huge industry that is worth over USD 745 billion [76]was predicted to increase to billions of connected devices by 2020 [10]. This brings great potential for both businesses and academia [21]. However, the more IOT applications are weaved into the fabric of everyday life, the more security concerns will be raised; which if neglected could threaten its existence [3].

2.1. IOT in Human Resources Management

Human resources (HR) are treated as strategic assets to achieve its sustainable competitive advantages. In human resources processes and practices, Information Technology has had a substantial effect [74]. The technological advancements have brought up the term terms Electronic Human Resource Management (E-HRM). E-HRM is being the facets of intranet based human resource management, virtual human resource management; website based human resource management and information system based upon the human resource management [11].Human Resource Management (HRM) refers to the strategic effort by management systems to plan, recruit, select, train and develop employees in order to achieve organisational and individual objectives [48]. The appreciation of society to the new technology trends forced organisations to adapt to more innovative solutions in order to suit the marketplace. Similarly, human resource professionals; who are also urged to keep up with these innovations in their practices [82] [13], have recognized e-HRM, which has become the pivot of human capital management solutions. Accordingly, HRM practices have also been re-defined as e-Recruitment, e-Payroll, e-Performance Management, e-Training etc.[13].

The influence of technology adoption derives change to the HR business process. Digitalization enables HRM to achieve its main objectives efficiently [9]. The excessive use of smart phones and cloud-based applications have changed the workplace and enabled organisations to perform work schedules with open work spaces or virtual workplace. IOT can transform HRM and allow organisations to take suitable HR decisions and promote organisational growth through the availability of easy and cost-effective employee data. This can be done through the establishment of systems to connect, track and measure the effectiveness and efficiency of humans in the digital work environment [13].IOT applications in HRM aim at improving HR practices, namely; HR analytics, recruitment, deployment, performance management, training and development, and compensation. IOT enables HRM to collect real-time big data. The sensing function of smart things stimulates changes and provides HRM with the strategies necessary to maximize agility and correct creation of workforce. For example, using wearable devices all employee-related information from diet, sleep, movements and pulse are monitored. Such data can be utilised to enhance productivity [73]. Utilising IOT in HRM can also digitize employees' attendance; where biometric systems are used to calculate the total working hours instantly. Compensation can thus be automatically calculated and debited to employees' bank accounts instantly and accurately [30][59]. IOT facilitates sending/retrieving employees' data, which improves performance appraisal and enhances delivering employees' benefits as promotion, salary increase, gifts, recognition, certificates etc.[78] and [73].

2.2. IOT Challenges

IOT continues to steer operations in the 21st century, numerous challenges are coming to light [59]. The first and most critical obstacle to IOT implementation is Security, which it considered as top priority [39]. This challenge is important due to the billions of devices connected through IOT; it requires an efficient security mechanism [59][49][5]. The security problem is magnified by the fact that many IOT devices may be built by companies that have little expertise in security [7][15][50]. Considering challenges such as security is still important to enhance IOT adoption [61].Information security is a social and organizational problem because technical systems must be operated and used by people [22, p.7], which includes factors as confidentiality, integrity and availability of information achieved through the application of certai n standards and measures and organisational support for the preparation, implementation, andveri fication and updating of business standards and measures [56][29]. Also, information security is impacted by the individuals that use it and the same technologies that

Enable it to takeplace in compliance with these processes. The growing influence of information security policy thinking shows the width and scope of the content being protected [29]. According to the information security life cycle developed by [47], it is extremely significance for the organization to recognize that the process is never-ending, and the organization needs to improve its behaviour during every cycle. Information security is needed because the technology applied to information creates risks. When information security risk is recognized, it is necessary to create a policy for information security. These policies can be divided into four categories: protection measures, detection measures, consequences response measures and measures to ensure the effectiveness of the consequences response. Management uses information security policy to distinguish between employee behaviours that are either allowed or prohibited, as well as the corresponding penalties if the prohibited behaviours occur [22]. In order to ensure that the security policy is in line with standard organisational practices, it is critical that the human resource department be involved in the security policy development life cycle [53]. In this way, consistency between the organisation's security policy and standard organisational practices will be assured. According to [25] security policy should not have conflict with human resources policy.

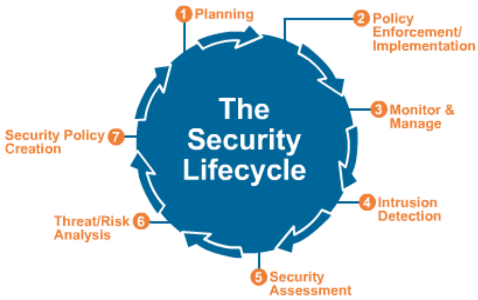

Figure 1. Information security life cycle [53, p. 123]

Software complexity in IOT cannot be neglected, where a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide supporting services, because software systems in smart objects will have to function with minimal resources, as unconventional embedded systems [19][68][67][49] [31].The presence of clear and strong IOT regulations is very important as well; it can decrease the fear of security breaches from IOT usage [16][51] [43]. Business policies and procedures create some social challenges to IOT and government laws, and rules pose legal challenges to its use [43]. IOT regulatory problem are amplified since the rapid rate of change in IOT technology outpaces the ability of the associated policy, legal, and regulatory structures to adapt [64]. If a government imposes IOT policy compliance with penalties on firms who do not comply, numerous organizations would be interested in IOT adoption [61].

Software development is an important challenge as well; as it is assumed that human lives will totally depend on things around them that are connected to the Internet, the validity and reliability of the data being sent and the decision taken accordingly is an equally important [85]. Challenges increase if the data sent is critical for human lives as heart beat rate or blood pressure for example. An IOT integration framework exclude all complexities and provide appropriate documentation for non-developers and developers with basic programming knowledge to understand the internals of the framework easily [77]. In other words, software developers must develop easy programs with high accuracy to guarantee decisions taken by things accordingly. Complex dependencies must also be considered [8]. Human behaviour in general is very complex that is influenced by a lot of variables. This makes its interpretation using software and sensors a real challenge. With IOT humans are able to monitor and control physical processes while interacting with very large data sets collected via sensors. For IOT to gain maximum efficiency and make human lives much easier software designed for sensors must be smart enough to take critical decisions and avoid conflict situations [75]. The presence of a lot of complexities will affect IOT adoption negatively [61].Perceived Safety is the degree to which a user believes that using a particular IOT system he would be free from possible dangers (health, physical, mental, financial, social, environmental, etc.), risks, losses, negative outcomes that can be caused from its usage. IOT products need to obtain software updates and security patches in a manner that preserves their limited bandwidth and connectivity and reduces the risk of sacrificing functional safety [32].

All of the above-mentioned challenges are assumed to affect how IOT is perceived. Perceived privacy risk plays a key factor in IOT adoption [38]. Therefore, ensuring security in IOT products and services should be considered a top priority [63]. Businesses aim to be more efficient and responsive by having a better control through strong governance, better communication, efficient coordination and cumulative vision of the organisation [72]. The intent for IOT adoption is another primary factor in the study of IoT.Technology readiness positively impacts IOT adoption[61].The unified theory of acceptance and use of technology (UTAUT) is an advanced tool developed to analyse and understand the factors that influence the acceptance of IOT [79][57]. The integrated model is the result of a combined eight models [80] and is one of the most popular frameworks in the field of technology acceptance models [81]. Some of the models incorporated are: Theory of Reasoned Action (TRA), Theory of planned behaviour (TPB), Technology acceptance models (TAM), and Motivational models (MM). There are four constructs / variables which are direct determinants of acceptance and use behaviour, the four variables are Social Influence (SI), Effort Expectancy (EE), Facilitating Conditions (FC), and Performance Expectancy (PE).Readiness to IOT applications has a great potential to revolutionize human capital management in the digital environment [13]. However, organisations need to acquaint employees with IOT and determine the key challenges to transforming from legacy systems to IOT enabled systems [84].Employee readiness to use IOT technology is not yet fully explored.

2.3. IOT in Organisations

With the arrival of IOT in organisations, it becomes more necessary to consider its potential proliferation and adapt correct strategies while investigating its attractiveness from the various perspectives. Those perspectives include, employees who are interested in the adoption of smart technology; the decision makers interested in increasing effectiveness and reducing administrative efforts; and the administrators who have administration obligations in managing the process. Assuming the arrival of IOT to organisation premises entails investigating the different perspectives in needs, readiness, or posing threats [27]. IOT can be used outdoors or indoors and can be used in the normal daily life activities. Employees check in and out through RFID tag identifiers and Smartphone applications generating attendance reports, where decision makers and administrators get automatic updates. Adding IOT to gateways of any campus/organisational premises helps in attaining security and reducing time wasted in checking employees' identification proofs/cards. Therefore, IOT helps in saving not only time but also avoids wastage of energy [27].

Many organisations still use ID (employee card) to check in and out; which has many limitations such as the processing time, where the card is inserted into a reader, processed, data read, and the employee is successfully identified. This process takes time and causes crowds and frustration. Moreover, these ID cards can be scratched, bent, or even lost. They may also be kept in wallets or pockets for long hours, and therefore the electromagnetic chip maybe affected. Not to mention the likelihood of typical human errors. Therefore, IOT are positively related to both growth and competitiveness [33]. IOT has a great impact in all major industries including the Banking and Financial Services sector; as it measures and provides useful quantified data, which can be analysed to ensure improved performance at workplace. Thus, it has become increasingly important for HR to automate the monitoring of the human productivity in terms of meaningful data and help them in making strategic decision making not only limited to clients' efficiency but have extended its dimensions to improve organisational efficiency [13].

2.4. The Egyptian Banking Industry

The Egyptian banking sector is considered one of the most developed in the Middle East and North Africa region. Therefore, the purpose of banking operations is supposed to enhance the quality of life for the overall society not just maximize shareholders' wealth [26]. The banking system in Egypt is a national priority; where it has been experiencing a clear increase in the number of customers using online banking services, with Internet users in Egypt reaching 49,231,493 million in March 2019; which brings Internet penetration to 48.7 % [86]. This justifieswhy the Egyptian economy heavily relies on the banking industry to maintain its stability. The banking industry in Egypt consists of a variety of segments [1], where there are commercial banks that accept deposits and provide finance for a wide variety of transactions; business and Investment banks that perform medium-and-long-term business and finance operations; and specialized banks which offer specific types of economic activities and accept demand deposits[40]. However, they have a significant contribution in the financial sector of the country [2][41][42].

3. RESEARCH FRAMEWORK AND HYPOTHESES

Despite the wide availability of studies on key dimensions that affect readiness to IOT applications, levels of importance remain variable between countries. Not to mention that only few studies focused on the banking industry. Accordingly, literature was extensively reviewed to derive the main dimensions that affect readiness to IOT applications in the Egyptian banking industry and propose the research framework; as illustrated in Fig. 1. The model contains research variables, that were highlighted in a variety of studies, namely: 'Networking', 'Software Development', 'Complex dependencies' and 'Regulations' and are considered antecedents to 'readiness to IOT applications'. Accordingly, the first hypotheses 1 to 5 were devised to test whether these factors still stand as the main factors within the context.

Since only few studies investigated factors that affect readiness to IOT applicationsin banks[60], and almost negligible investigations on mediating and moderating factors, 'Security' and Intention to Use' are proposed by the researchers as mediators for the relationship between the research variables and the 'readiness to IOT applications'. This assumption was based on the fact that a variety of investigations have revealed that Security is the most critical obstacle. Thus, it was worth investigating its mediating effect to test whether with its absence, other independent dimensions would still affect the readiness to IOT applications. This also applies to the user intention, which was proven as a prerequisite to readiness to IOT applications. Therefore, hypothesis 6 was devised to test their mediating impact on the model.'Efficiency' was introduced as a moderator for the model, in order to examine whether its importance stems from its impact on strengthening the relationship between the research variables and the readiness to IOT applications. Thus, hypothesis 7 was devised to test the 'Efficiency' moderating role. To the best of the researchers' knowledge, this study is the first to investigate mediating and moderating factors in the Egyptian banking context; especially in the pandemic, which makes technology adoption a calling need, rather than just an interesting trend with great potential.

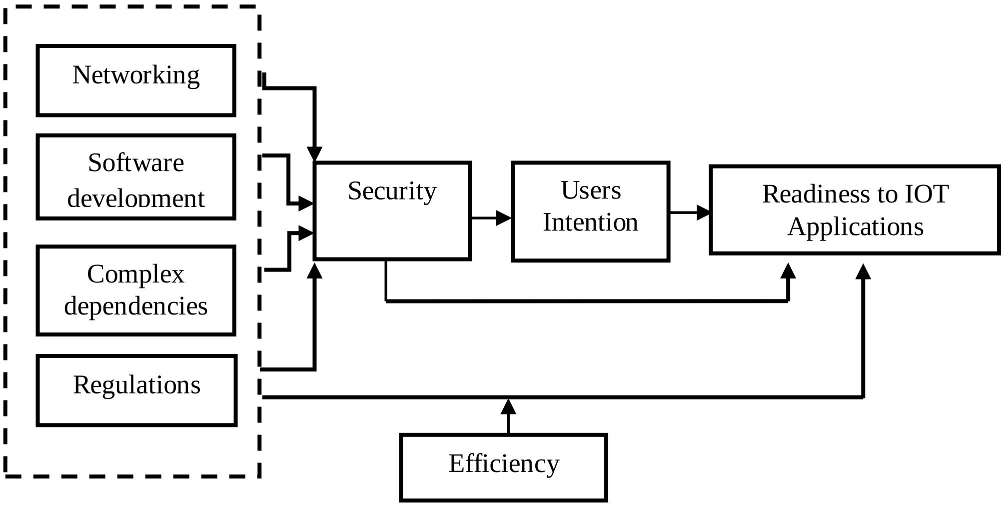

Figure 2. Proposed Research Model for Readiness to IOT Applications

Therefore, the four constructs mentioned above are considered as the factors affecting the Readiness to IOT applications in Egypt, and they are mediated by Security and Users' Intention, and moderated by Efficiency. Thus, the research hypotheses could be developed as follows:

H1: There is a significant impact of Research variables on Readiness to IOT applications.
H1.1: There is a significant impact of Networking on Readiness to IOT applications.
H1.2: There is a significant impact of Software development on Readiness to IOT applications.
H1.3: There is a significant impact of Complex dependencies on Readiness to IOT applications.
H1.4: There is a significant impact of Regulations on Readiness to IOT applications.
H2: There is a significant impact of Research variables on Security.
H2.1: There is a significant impact of Networking on Security.
H2.2: There is a significant impact of Software development on Security.
H2.3: There is a significant impact of Complex dependencies on Security.
H2.4: There is a significant impact of Regulations on Security.
H3: There is a significant impact of Security on Users' Intention.
H4: There is a significant impact of Security on Readiness to IOT applications.
H5: There is a significant impact of Users' Intention on Readiness to IOT applications.
H6: Security and Users' Intention mediate the relationship between Research variables and Readiness to IOT applications.
H6.1: Security mediates the relationship between Research variables and Readiness to IOT applications.
H6.2: Users' Intention mediates the relationship between Research variables and Readiness to IOT applications.
H7: Efficiency moderates the relationship between Research Variables and Readiness to IOT applications.
H7.1: Efficiency moderates the relationship between Networking and Readiness to IOT applications.
H7.2: Efficiency moderates the relationship between Software development and Readiness to IOT applications.
H7.3: Efficiency moderates the relationship between Complex dependencies and Readiness to IOT applications.
H7.4: Efficiency moderates the relationship between Regulations and Readiness to IOT applications.

4. DATA COLLECTION AND ANALYSIS

To test the hypotheses, a survey was conducted to investigate the impact and adoption of Internet of Things in HRM at banks in Egypt. The Items used to test the constructs are mainly adapted from previous studies. A structured questionnaire is designed as shown in Appendix, where questionnaire items are adopted and adapted to suit the study's context. The questionnaire is designed in English and translated into Arabic, containing 47 statements regarding various aspects of IOT. A five-point Likert scale is used to capture the level of agreement with each statement. Questionnaire forms are randomly distributed in both languages, according to respondents' preferences over 700 employees at banks in Egypt. Data was collected on four months duration (March 2020 – July 2020).Data collected was coded and analysed using SPSS and AMOS to compute the reliability, validity, descriptive statistics and regression analysis to test the research hypotheses. In order to confirm the overall structure of the research model, the structural equation modelling (SEM) technique [55] [66] was applied. This section presents the data analysis in order to test the research hypotheses. For data testing, convergent validity is measured by the two main factors; the Average Variance Extracted (AVE) and the factor loading (FL). AVE represents the average community for each latent factor, which has to be greater than 0.5 to assume adequate validity. Second is the factor loading for each item, which should be greater than or equal to 0.4 to imply adequate validity [44]. Table 1 shows the convergent validity test of the variables under study, namely; Networking, Software development, Complex dependencies, Regulations, Security, User intention and Readiness to IOT applications, where all AVE values corresponding to the mentioned variables exceed 50% and all FL values exceed 0.4.To examine reliability, each factor is measured using a group of statements, where the consistency between these statements refers to their reliability in which it can be examined by Cronbach's Alpha; the most common used test of reliability. The adequate reliability should be referred by Alpha coefficients exceeding 0.7. Table 1 shows the reliability test of the research variables, where all alpha coefficients are found to be greater than 0.7, implying adequate reliability.

Table 1.Validity and Reliability Test

Variables	**KMO**	**AVE**	**Cronbach's Alpha**	**Items**	**FL**
Networking	.835	59.280%	.828	Item1	.541
				Item2	.652
				Item3	.594
				Item4	.545
				Item5	.632
Software Development	.681	70.405%	.784	Item1	.680
				Item2	.777
				Item3	.655
Complex Dependencies	.830	62.622%	.850	Item1	.561
				Item2	.621
				Item3	.645
				Item4	.628
				Item5	.677
Regulations	.882	69.287%	.910	Item1	.689
				Item2	.706
				Item3	.725
				Item4	.645
				Item5	.696
				Item6	.696
Security	.584	64.420%	.714	Item1	.442

Variables	KMO	AVE	Cronbach's Alpha	Items	FL
				Item2	.798
				Item3	.692
User intention	.894	48.903%	.868	Item1	.481
				Item2	.431
				Item3	.564
				Item4	.478
				Item5	.464
				Item6	.505
				Item7	.492
				Item8	.555
				Item9	.432
Efficiency	.814	64.447%	.862	Item1	.597
				Item2	.710
				Item3	.630
				Item4	.609
				Item5	.677
Readiness to IOT applications	.729	80.693%	.879	Item1	.837
				Item2	.832
				Item3	.751

Descriptive analysis provides summary statistics about the research variables, including the mean and standard deviations. Table 2 shows the descriptive analysis for the research variables, where it could be observed that the mean of the research variables; Networking, Software development, Complex dependencies, Regulations, Security, User intention, Efficiency and Readiness to IOT applications are 4.0418, 3.8559, 4.0230, 3.7035, 4.1962, 4.0689, 4.0731, and 4.0146 respectively.

Table 2. Descriptive Analysis for Research variables

Research Variables	N	Mean	Std. Deviation	Frequency				
				1	2	3	4	5
Networking	479	4.0418	.62239	0	0	83	293	103
Software development	479	3.8559	.61885	0	0	131	286	62
Complex dependencies	479	4.0230	.63830	0	0	92	284	103
Regulations	479	3.7035	.58913	0	0	175	271	33
Security	479	4.1962	.54418	0	0	33	319	127
User intention	479	4.0689	.54259	0	0	55	336	88
Efficiency	479	4.0731	.70628	0	0	107	258	114
Readiness to IOT applications	479	4.0146	.67980	0	0	103	238	138

Normality testing is important for determining the tests to be used in the research. In order to check the normality for the data, two types of tests are conducted; formal and informal testing. Table 3 shows the formal testing of normality assumption for the research variables conducted by the Kolmogorov-Smirnov test of normality. It could be observed that the research variables are not exactly normally distributed, as the corresponding P-values are less than 0.05, implying that the skewness and kurtosis values are not equal to zero.

Table 3. Formal Testing of Normality

	Kolmogorov-Smirnov		
	Statistic	**df**	**P-value**
Networking	.312	479	.000
Software Development	.319	479	.000
Complex Dependencies	.299	479	.000
Regulations	.327	479	.000
Security	.376	479	.000
User intention	.367	479	.000
Internet of Things	.253	479	.000
Efficiency	.271	479	.000

As the formal test shows that the research variables are not normally distributed, an informal test could be used to detect the approximate normality, as the sample size is greater than 150. Table 4 shows the informal test of normality, where it could be shown that the skewness and kurtosis values are within the accepted level of ±1. This means that the data under study are approximately normal.

Table 4. Informal Testing of Normality

	N	Skewness		Kurtosis	
	Statistic	**Statistic**	**Std. Error**	**Statistic**	**Std. Error**
Networking	479	-.028	.112	-.413	.223
Software Development	479	.102	.112	-.467	.223
Complex Dependencies	479	-.020	.112	-.535	.223
Regulations	479	.185	.112	-.589	.223
Security	479	.092	.112	-.095	.223
User intention	479	.049	.112	.353	.223
Internet of Things	479	-.104	.112	-.989	.223
Efficiency	479	-.018	.112	-.828	.223

Accordingly, the researcher is able to use the Pearson correlation, regression analysis as well as the SEM analysis. The following shows the hypotheses testing using the assigned statistical tests.

H1: Testing the Effect of Independent variables on Readiness to IOT applications

Table 5 shows the correlation matrix between the independent variables; Networking, Software development, Complex dependencies, Regulations, and Readiness to IOT applications. It was observed that the values of Pearson's correlation for the research variables; Networking, Software development, Complex dependencies, Regulations, and Readiness to IOT applications are 0.683, 0.575, 0.651, and 0.364 respectively. Therefore, it could be claimed that there is a significant positive correlation between the research variables and Readiness to IOT applications, as corresponding P-values are less than 0.05 and $r > 0$.

Table 5. Correlation Matrix between independent variables on Readiness to IOT applications

		1	2	3	4	5
1. Networking	Pearson Correlation	1				
	Sig. (2-tailed)					
	N	479				
2.Software development	Pearson Correlation	.591**	1			
	Sig. (2-tailed)	.000				
	N	479	479			
3.Complex dependencies	Pearson Correlation	.624**	.464**	1		
	Sig. (2-tailed)	.000	.000			
	N	479	479	479		
4. Regulations	Pearson Correlation	.291**	.319**	.274**	1	
	Sig. (2-tailed)	.000	.000	.000		
	N	479	479	479	479	
5.Readiness to IOT applications	Pearson Correlation	.683**	.575**	.651**	.364**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	479	479	479	479	479

Table 6 shows the multiple regression analysis of the influence of the independent variables; Networking, Software development, Complex dependencies, Regulations on Readiness to IOT applications. It was found that the P-values corresponding to the research variables; Networking, Software development, Complex dependencies and Regulations are 0.000, 0.000, 0.000 and 0.000. Also, the coefficients are 0.383, 0.216, 0.354 and 0.141 respectively, implying a positive significant impact of the research variables on Readiness to IOT applications. However, the R square is 0.590 which means that the model explains 59% of the variation in Readiness to IOT applications. Thus the first hypothesis is accepted.

Table 6. Regression Model of Independent Variables Effect on Readiness to IOT applications

	Unstandardized Coefficients		Standardized Coefficients			
Model	B	Std. Error	Beta	T	P-value	R-Square
(Constant)	-.254	.178		-1.431	.153	
Networking	.383	.048	.337	8.044	.000	.590
Software development	.216	.043	.189	5.047	.000	
Complex dependencies	.354	.042	.320	8.365	.000	

H2: Testing the Effect of Independent variables on Security

Table 7 shows the correlation matrix between the independent variables; Networking, Software development, Complex dependencies, Regulations, and Security. It was observed that the values of Pearson's correlation for the research variables; Networking, Software development, Complex dependencies, Regulations, and Security are 0.507, 0.475, 0.481, and 0.332 respectively. Therefore, it could be claimed that there is a significant positive correlation between the research variables and Security, as corresponding P-values are less than 0.05 and r > 0.

Table 7. Correlation Matrix between independent variables on Security

		1	2	3	4	5
1. Networking	Pearson Correlation	1				
	Sig.(2-tailed)					
	N	479				
2.Software development	Pearson Correlation	.591**	1			
	Sig. (2-tailed)	.000				
	N	479	479			
3.Complex dependencies	Pearson Correlation	.624**	.464**	1		
	Sig. (2-tailed-)	.000	.000			
	N	479	479	479		
4. Regulations	Pearson Correlation	.291**	.319**	.274**	1	
	Sig. (2-tailed)	.000	.000	.000		
	N	479	479	479	479	
5. Security	Pearson Correlation	.507**	.475**	.481**	.332**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	479	479	479	479	479

Table 8 shows the multiple regression analysis of the influence of Networking, Software development, Complex dependencies, Regulations on Security. it was found that P-values of the research variables; Networking, Software development, Complex dependencies and Regulations are all less than 0.05 and the coefficients are 0.182, 0.181, 0.183 and 0.136 respectively, implying a positive significant impact of the research variables on Security. Thus, the second hypothesis is accepted.

Table 8. Regression Model of Independent Variables on Security

	Unstandardized Coefficients		Standardized Coefficients		
Model	B	Std. Error	Beta	T	P-value
(Constant)	1.522	.172		8.873	.000
Networking	.182	.046	.208	3.963	.000
Software development	.181	.041	.206	4.378	.000
Complex dependencies	.183	.041	.215	4.486	.000
Regulations	.136	.036	.147	3.724	.000

H3: Testing the Effect of Security on User Intention

Table 9 shows the correlation matrix between Security and User intention. There is a significant positive correlation, as the corresponding P-value is less than 0.05 and Pearson's correlation coefficient is 0.599, which is greater than zero. Thus, the third hypothesis is accepted.

Table 9. Correlation Matrix between Security on User intention

		Security	User intention
Security	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	479	
User intention	Pearson Correlation	.599**	1
	Sig. (2-tailed)	.000	
	N	479	479

Table 10 shows the simple regression model of the influence of Security on User intention. It could be observed that there is a positive significant influence of Security on User intention with regression coefficient 0.597, as well as P-value of 0.000, which is less than 0.05.

Table 10. Regression Model of Security on User intention

Model	Unstandardized Coefficients		Standardized Coefficients	T	P-value
	B	Std. Error	Beta		
(Constant)	1.563	.155		10.105	.000
Security	.597	.037	.599	16.332	.000

H4: Testing the Effect of Security on Readiness to IOT applications

Table 11 shows the correlation matrix between Security and Internet of Things. There is a significant positive correlation, as the corresponding P-value is less than 0.05 and Pearson's correlation coefficient is 0.550, which is greater than zero.

Table 11. Correlation Matrix between Security on Internet of Things

		Security	User intention
Security	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	479	
Internet of Things	Pearson Correlation	.550**	1
	Sig. (2-tailed)	.000	
	N	479	479

Table 12 shows the simple regression model of the influence of Security on Internet of Things. It could be observed that there is a positive significant influence of Security on Internet of Things with regression coefficient 0.714, as well as P-value of 0.000, which is less than 0.05.Thus, the fourth is accepted.

Table 12. Regression Model of Security on Internet of Things

Model	Unstandardized Coefficients		Standardized Coefficients	T	P-value
	B	Std. Error	Beta		
(Constant)	1.075	.210		5.121	.000
Security	.714	.050	.550	14.401	.000

H5: Testing the Effect of User intention on Readiness to IOT applications

Table 13 shows the correlation matrix between User intention and Readiness to IOT applications. There is a significant positive correlation as the corresponding P-value is less than 0.05 and Pearson's correlation coefficient is 0.549, which is greater than 0.

Table 13. Correlation Matrix between User intention and Readiness to IOT applications

		User intention	Internet of Things
User intention	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	479	
Internet of Things	Pearson Correlation	.549**	1
	Sig. (2-tailed)	.000	
	N	479	479

Table 14 shows the simple regression model of the influence of User intention on Readiness to IOT applications. It could be observed that there is a significant influence of User intention on Readiness to IOT applications with regression coefficient 0.715, as well as P-value of 0.000, which is less than 0.05. Thus, the fifth is accepted.

Table 14. Regression Model of User intention on Readiness to IOT applications

	Unstandardized Coefficients		Standardized Coefficients		
Model	B	Std. Error	Beta	T	P-value
(Constant)	1.165	.204		5.696	.000
User intention	.715	.050	.549	14.350	.000

H6: Testing Security and User's Intention mediate the relationship between research variables and Readiness to IOT Applications

Table 15 show the regression model fitted for the mediation role of Security between Research Variables and Readiness to IOT applications. According to the results obtained from Table 6 it could be observed that the relation between Research Variables and Readiness to IOT applications are significant. Also, regarding the results from Table 12 it could be observed that the relation between Security and Readiness to IOT applications is significant, so, based on the results from Table 15 it could be noted that there is a significant effect of the Research Variables and Readiness to IOT applications with the existence of Security which is also has a significant effect. Further, the Security mediates the relation between the Research Variables and Readiness to IOT applications.

Table 15. Mediation Role of Security between Research Variable and Readiness to IOT applications

	Unstandardized Coefficients		Standardized Coefficients		
Model	B	Std. Error	Beta	T	P-value
(Constant)	-.550	.189		-2.918	.004
Networking	.347	.048	.306	7.304	.000
Software Development	.181	.043	.158	4.212	.000
Complex Dependencies	.318	.042	.288	7.494	.000
Regulations	.115	.038	.096	3.057	.002
Security	.194	.047	.150	4.160	.000

Table 16 show the regression model fitted for the mediation role of User intention between Research Variables and Readiness to IOT applications. According to the results obtained from Table 6 it could be observed that the relation between Research Variables and Readiness to IOT applications are significant. Also, regarding the results from Table 14 it could be observed that the relation between User intention and Readiness to IOT applications is significant, so, based on the results from Table 16 it could be noted that there is a significant effect of the Research Variables and Readiness to IOT applications with the existence of User intention which also has a significant effect. Furthermore, the User intention mediates the relation between the Research Variables and Readiness to IOT applications. Thus, the sixth hypothesis is accepted.

Table 16. Mediation Role of User intention between Research Variable and Readiness to IOT applications

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	T	P-value
(Constant)	-.619	.188		-3.301	.001
Networking	.335	.047	.295	7.066	.000
Software Development	.190	.042	.166	4.511	.000
Complex Dependencies	.311	.042	.281	7.388	.000
Regulations	.116	.037	.097	3.131	.002
User intention	.228	.045	.175	5.059	.000

H7: Testing Efficiency Moderation between Independent Variables and Readiness to IOT applications.

Table 17 shows the regression model fitted for the moderation role of Efficiency between Networking and Readiness to IOT applications. It was found that there is a significant moderation of Efficiency between Networking and Efficiency as the P-value is less than 0.05 and correlation coefficient is -0.119.

Table 17. Moderation Role of Efficiency between Networking and Readiness to IOT applications

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	P-value
(Constant)	-1.219	1.005		-1.214	.225
Networking	1.212	.249	1.068	4.867	.000
Efficiency	.587	.248	.565	2.366	.018
Network * Efficiency	-.119	.060	-.779	-1.993	.047

Testing the Efficiency moderation between Software development and Readiness to IOT applications: Table 18 shows the regression model fitted for the moderation role of Efficiency between Software development and Readiness to IOT applications. It was found that there is a significant moderation of Efficiency between Software development and Efficiency as the P-value is less than 0.05 and correlation coefficient is -0.251.

Table 18. Moderation Role of Efficiency between Software development and Readiness to IOT applications

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	P-value
(Constant)	-3.264	.941		-3.471	.001
Software development	1.620	.245	1.419	6.608	.000
Efficiency	1.247	.226	1.201	5.516	.000
Software Development * Efficiency	-.251	.058	-1.470	-4.323	.000

Testing the Efficiency moderation between Complex dependencies and Readiness to IOT applications: Table 19 shows the regression model fitted for the moderation role of Efficiency between Complex dependencies and Readiness to IOT applications. It was found that there is a significant moderation of Efficiency between Complex dependencies and Efficiency as the P-value is less than 0.05 and correlation coefficient is -0.119.

Table 19. Moderation Role of Efficiency between Complex dependencies and Readiness to IOT applications

Model	Unstandardized Coefficients		Standardized Coefficients	t	P-value
	B	Std. Error	Beta		
(Constant)	-1.037	.952		-1.089	.277
Complex dependencies	1.129	.235	1.021	4.799	.000
Efficiency	.626	.240	.602	2.610	.009
Complex Dependencies * Efficiency	-.119	.058	-.771	-2.061	.040

Testing the Efficiency moderation between Regulations and Readiness to IOT applications: Table 20 shows the regression model fitted for the moderation role of Efficiency between Regulations and Readiness to IOT applications. It was found that there is an insignificant moderation of Efficiency between Regulations and Efficiency as the P-value is more than 0.05 and correlation coefficient is 0.122.

Table 20. Moderation Role of Efficiency between Regulations and Readiness to IOT applications

Model	Unstandardized Coefficients		Standardized Coefficients	t	P-value
	B	Std. Error	Beta		
(Constant)	3.283	1.050		3.128	.002
Regulations	-.173	.289	-.144	-.600	.549
Efficiency	-.098	.252	-.094	-.390	.697
Regulations * Efficiency	.122	.068	.677	1.784	.075

Thus, the seventh hypothesis is partially accepted. Table 21 shows the SEM analysis of the influence of the research variables; Networking, Software development, Complex dependencies, Regulations on Readiness to IOT applications. It was found that the model fit indices; CMIN/df = 2.151, GFI = 0.921, CFI = 0.960, and RMSEA = 0.049 are all within their acceptable levels. It was also found that there is a significant influence of Networking, Software development, Complex dependencies, and Regulations on the Readiness to IOT applications with Estimates of 0.596, -0.193, 0.222 and 0.139 respectively, as well as the P-values are less than 0.05.

Table 21. SEM for Research Model

			Estimate	P
Readiness to IOT applications	<---	Networking	.596	***
Readiness to IOT applications	<---	Software development	-.193	.040
Readiness to IOT applications	<---	Complex dependencies	.222	.025
Readiness to IOT applications	<---	Regulations	.139	.034

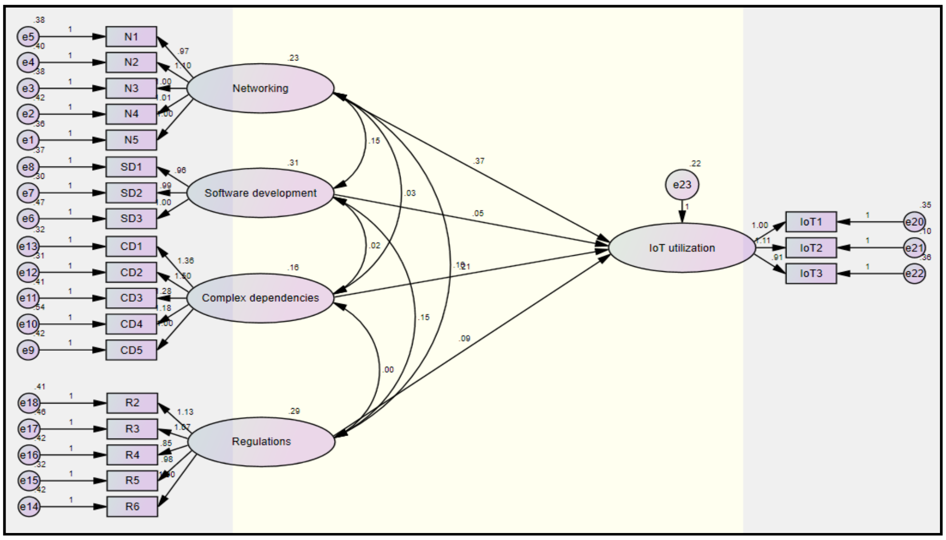

Figure 3. SEM Model for the Direct Impact on Readiness to IOT applications

Table 22 show the SEM analysis of the influence of the research variables; Networking, Software development, Complex dependencies, Regulations, Security, and User intention on Readiness to IOT applications. It was also found that there is a significant influence of Networking, and Regulations on Security with Estimates of 0.220 and 0.070 respectively, as well as the P-values are less than 0.05, while, there is a significant influence of Software development, Complex dependencies, and Regulations on User intention with Estimates of 0.199, 0.195 and 0.119 respectively, as well as the P-values are less than 0.05. Furthermore, there is a significant influence of Networking, Complex dependencies, and Regulations on Readiness to IOT applications with Estimates of 0.658, 0.313 and 0.155 respectively, as well as the P-values are less than 0.05. Also, it was found that the model the model fit indices are; CMIN/df = 1.625, GFI = 0.909, CFI = 0.961, and RMSEA = 0.036 are all within their acceptable levels.

Table 22. SEM for Research Model

			Estimate	P
Security	<---	Networking	.220	***
Security	<---	Software Development	.075	.069
Security	<---	Complex Dependencies	.088	.078
Security	<---	Regulations	.070	.019
Users Intention	<---	Networking	.129	.062
Users Intention	<---	Software Development	.199	***
Users Intention	<---	Complex Dependencies	.195	.006
Users Intention	<---	Regulations	.119	.004
Readiness to IOT appl.	<---	Networking	.658	***
Readiness to IOT appl.	<---	Software Development	-.153	.124
Readiness to IOT appl.	<---	Complex Dependencies	.313	.008
Readiness to IOT appl.	<---	Regulations	.155	.026
Readiness to IOT appl.	<---	Security	-.228	.157
Readiness to IOT appl.	<---	Users Intention	-.127	.223

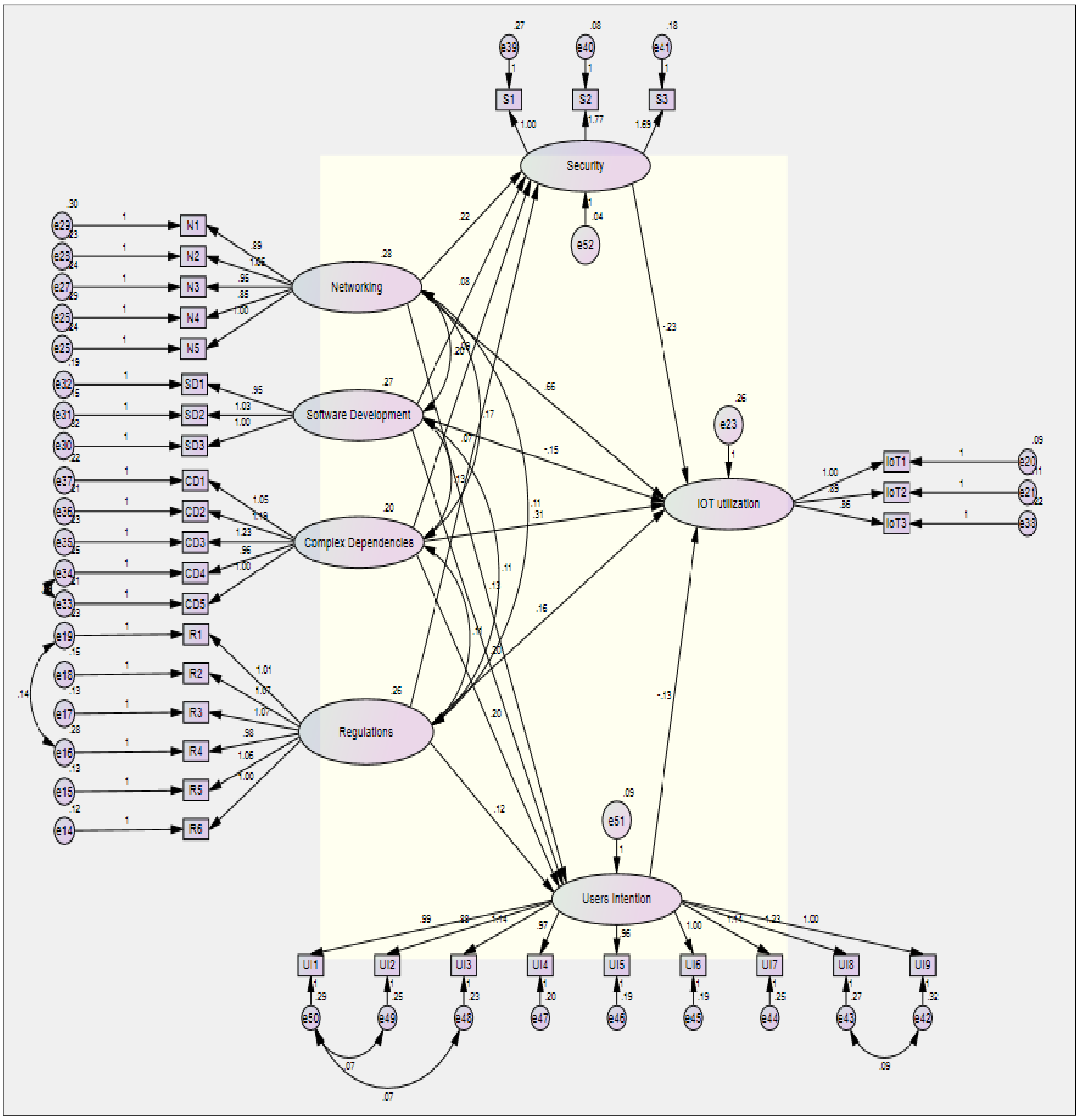

Figure 4. SEM Model for the Mediation Role of Security and User Intention

Table 23 show the SEM analysis of the influence of the whole model on Readiness to IOT applications. It was also found that there is a significant influence of research variables; Networking, Software development, Complex dependencies, and Regulations on Security with Estimates of 0.178, 0.059, 0.120 and 0.078 respectively, as well as the P-values are less than 0.05, while, there is a significant influence of Networking, Software development, Complex dependencies, and Regulations on User intention with Estimates of 0.158, 0.088, 0.253 and 0.112 respectively, as well as the P-values are less than 0.05. Furthermore, there is a significant influence of Software development, and Regulations on Readiness to IOT applications with Estimates of -0.143 and -0.421 respectively, as well as the P-values are less than 0.05. Also, it was found that the model fit indices are; CMIN/df = 1.790, GFI = 0.890, CFI = 0.962, and RMSEA = 0.041 are all within their acceptable levels.

Table 23. SEM for Research Model

			Estimate	P
Security	<---	Networking	.178	***
Security	<---	Software Development	.059	.014
Security	<---	Complex Dependencies	.120	.001
Security	<---	Regulations	.078	.008
User intention	<---	Networking	.158	***
User intention	<---	Software Development	.088	.008
User intention	<---	Complex Dependencies	.253	***
User intention	<---	Regulations	.112	.006
Readiness to IOT applications	<---	Networking	-.217	.390
Readiness to IOT applications	<---	Software Development	-.143	.025
Readiness to IOT applications	<---	Complex Dependencies	-.086	.773
Readiness to IOT applications	<---	Regulations	-.421	***
Readiness to IOT applications	<---	Security	.092	.159
Readiness to IOT applications	<---	User intention	-.035	.418
Readiness to IOT applications	<---	N.E	.065	.197
Readiness to IOT applications	<---	SD.E	.036	.016
Readiness to IOT applications	<---	CD.E	.028	.561
Readiness to IOT applications	<---	R.E	.090	***

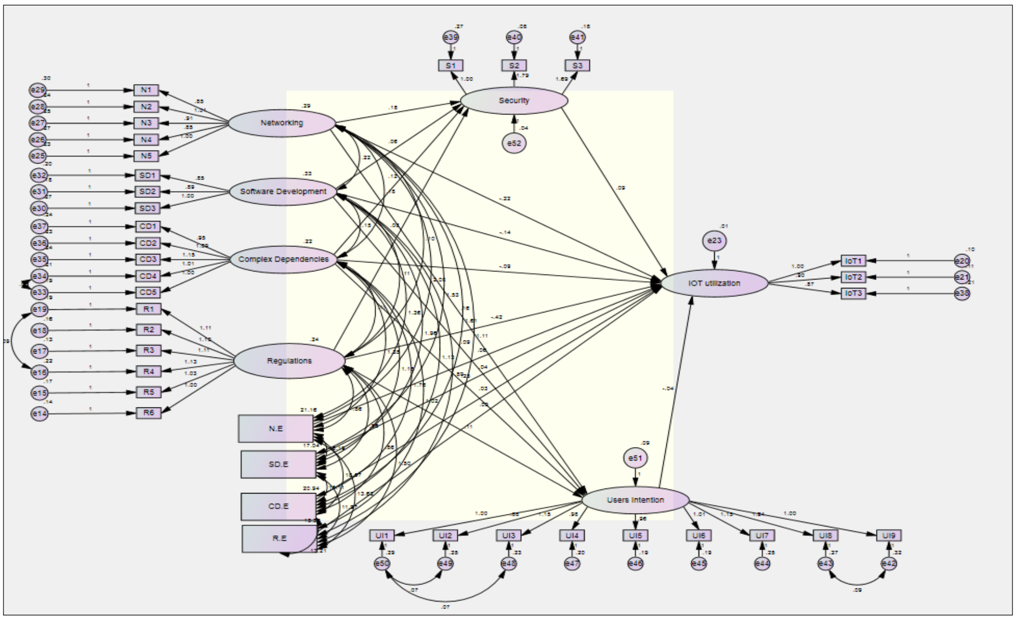

Figure. 5. SEM Model for the whole model

5. CONCLUSION

Internet of Things is the fastest growing new technology that we perceive in the present world. IOT provides many applications to identify and connect objects to each other through the Internet. Although its potential is obvious in transforming the way organisations conduct business, yet it did not dominate in organizations; especially in HRM practices. This research thoroughly investigated Readiness to IOT applications through an extensive review of literature and conducting a survey in order to identify the main factors affecting Readiness to IOT applications in the Egyptian banking industry, while determining the mediating and moderating factors involved in the research model. Results proved that there is a significant positive impact of ‘Networking’, ‘Software Development’, ‘Complex Dependencies’ and ‘Regulations’ on ‘Readiness to IOT applications’. These results clearly match the literature found regarding those variables and their effect on employee readiness [16] and [44]. Although few studies investigated factors that affect readiness to IOT applications in banks, and almost negligible investigations were done on mediating and moderating factors, ‘Security’ and ‘User intention’ proved to affect the readiness to using IOT [7] [15] [50]. Results showed that ‘Security’ and ‘User intention’ significantly mediate the relationship between ‘Networking’, ‘Software Development’, ‘Complex Dependencies’ and ‘Regulations’ and ‘Readiness to IOT applications’. Literature showed that businesses aim to be more efficient and responsive by having a better control through strong governance, better communication, efficient coordination and cumulative vision of the organisation [71].‘Efficiency’ was introduced as a moderator for the model, in order to examine whether its importance stems from its impact on strengthening the relationship between the research variables and the readiness to IOT applications. ‘Efficiency’ was found to have a significant impact on ‘Readiness to IOT applications’, with R Square of 0.59, which is relatively large contribution of ‘Efficiency’ in the variation of ‘Readiness to IOT applications’. Efficiency was also found to play a partial significant moderation role between the independent research variable together with ‘Readiness to IOT applications’.

5.1. Theoretical Contributions

The current study examined the determining factors of employees’ readiness to IOT applications in the Egyptian banking industry. The study’s results not just test and confirm that the main factors affecting readiness to IOT applications identified in literature, still stand in the Egyptian banking context, but also indicate that ‘Security’ and ‘User intention’ are mediating factors that explain the relationship between the independent research variables and the readiness to IOT applications. Based on the statistical analysis, although users tend to be more ready to IOT applications if ‘Networking’, ‘Software Development’, ‘Complex dependencies’ and ‘Regulations’ were maintained, ‘Security’ and ‘Users Intention’ play a mediating role. The study also proves the moderating role of ‘Efficiency’; which implies that ‘Efficiency’ strengthens the relationship between all independent variables except ‘Regulations’, and IOT applications’ readiness.

5.2. Research Contributions

This study contributes to the understanding of readiness to IOT applications by identifying the mediating role of ‘Security’ and ‘Users Intention’, and the moderating role of ‘Efficiency’. The study also contributes to fills a gap on the Egyptian banking context in particular. Finally, it provides a building block for further academic investigations as proposed in the study’s future work. In addition to its theoretical relevance, this study has several practical implications. IOT applications have great potential to facilitate banking transactions. In order to ensure unlocking its full potential, it must be perceived as a secure method for transactions. The present study’s results can provide decision makers at banks with useful guidelines on how to optimally promote IOT applications among employees. For example, the findings revealed that perceived security with IOT applications is a determining driver to readiness to IOT applications. Since new security challenges will always arise, keeping the entire linked banking experience safe and secure is crucial to gain user trust. This implies that while creating awareness and motivating employees to engage, decision makers should emphasize the security of transactions. The study also emphasizes the mediating role of 'User intention'; this could be a clear indication to decision makers that users will not be ready to IOT applications unless they are motivated by key factors in order to enhance user intention. Thus, key drivers will not have the required impact, except through 'User Intention' together with 'Security'. On the other hand, the partial moderating role of 'Efficiency' proven by the study should be the base to decision makers and practitioners when implementing IOT applications. The study highlights the importance of efficiency in IOT applications; as it positively enhances the relationship between 'Networking', 'Software Development', and 'Complex Dependencies' on one side and readiness to IOT applications on the other. Finally, this investigation should pave the way to decision makers and practitioners

5.3. Research Limitations and Future Work

The current research faced a number of limitations. The lack of data on IOT in the Egyptian banking context, did not allow room for conducting a comparative study between studies conducted in Egypt compared to those on a different context. Moreover, questionnaires were only distributed over employees at banks. It is recommended that the model should be tested across various sectors other than the banking industry. A longitudinal study may also reveal different results. Furthermore, the study only investigated the perspective of HR employees; a stakeholder analysis may reveal similarities or differences. Finally, the model explains 59% of the variations of Readiness to IOT applications in HRM, other factors that may affect Readiness to IOT applications could be worth investigating in order to have a more comprehensive study.

REFERENCES

[1] Abd El Aziz, R., Beeson, I., and Hussien, M. I. (2018), "A Soft Systems Methodology Based Analysis of the ATM System in Egypt", International Journal of Computer and Information Technology (ISSN: 2279 – 0764) 7(4), 176 – 183.

[2] Abd El Aziz, R., El Badrawy, R., and Hussien, M. I. (2014). 'ATM, Internet Banking and Mobile Banking Services in a Digital Environment: The Egyptian Banking Industry'. International Journal of Computer Applications, 90 (8).

[3] Abed A.H., Nasr M., Sayed B. (2020), 'The Principle Internet of Things (IoT) Security Techniques Framework Based on Seven Levels IoT's Reference Model'. In: Ghalwash A., El Khameesy N., Magdi D., Joshi A. (eds) Internet of Things—Applications and Future. Lecture Notes in Networks and Systems, 114. Springer, Singapore, pp 219-237, 978-981-15-3074-6

[4] Abdelmoumen, R. (2019). A Review of Link Layer Protocols for Internet of Things. International Journal of Computer Applications, 182 (46), 0975 – 8887.

[5] Alhalafi, N and Veeraraghavan, P. (2019). Privacy and Security Challenges and Solutions in IOT: A review. International Conference on Smart Power and Internet Energy Systems. doi:10.1088/1755-1315/322/1/012013.

[6] AlHogail, A. (2018). Improving IOT Technology Adoption through Improving Consumer Trust, Technologies, 6(4).

[7] Ali, I. Sabir,s and Ullah, Z. (2016). Internet of Things Security, Device Authentication and Access Control: A Review. International Journal of Computer Science and Information Security, 14, 456.

[8] Alur, R., Berger, E., Drobnis, A. W., Fix, L., Fu, K., Hager, G. D., Lopresti, D., Nahrstedt, K., Mynatt, E., Patel Sh., Rexford, J., Stankovic, J A., and Zorn, B (2016). Systems computing challenges in the Internet of Things. Computing Community Consortium.

[9] Angrave, D., Charlwood, A., Kirkpatrick, I., Lawrence, M., and Stuart, M. (2016). HR and analytics: why HR is set to fail the big data challenge. Human Resource Management Journal, 26(1), 1-11.

[10] Arshad, R, Zahoor S, Shah MA, Wahid A, Yu H (2017) Green IoT: An investigation on energy saving practices for 2020 and beyond. IEEE Access 5:15667–15681

[11] AzharNaima, M. (2019).Factors Affecting the Acceptance of E-HRM in Iraq. International Journal of Academic Research in Business and Social Sciences, 9(2)., 265-276.

[12] Banga, K., and teVelde, D. W. (2018). Digitalisation and the Future of Manufacturing in Africa.

[13] Barman, A., Das. K. (2018). Internet of Things (IOT) as the Future Smart Solution to HRM-How would wearable IOT bring organisational efficiency? Introduction: Rise of HR Technology. International Conference Dec, 2018 organised by RDA at Sibsagar, Assam.

[14] Bibri S. (2020) TheIoT and Big Data Analytics for Smart Sustainable Cities: Enabling Technologies and Practical Applications. In: Advances in the Leading Paradigms of Urbanism and their Amalgamation. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham, pp 191-226.

[15] Bilal, M. (2017). A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. arXiv preprint arXiv:1708.04560.

[16] Brass, I., Tanczer, L., Carr, M., Elsden, M., and Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security Standards, 1-9.

[17] Burhanuddin, M. A., Mohammed, A. A. J., Ismail, R., and Basiron, H. (2017). Internet of Things Architecture: Current Challenges and Future Direction of Research. International Journal of Applied Engineering Research, 12(21), 11055-11061.

[18] Castells, M. and Castells, M. (1971), The rise of the network society, 2nd ed., With a new pref. Chichester, West Sussex ; Malden, MA: Wiley-Blackwell, 2010.

[19] Charmonman, S., Mongkhonvanit, P., Dieu, V., and Linden, N. (2015). Applications of internet of things in e-learning.International Journal of the Computer, the Internet and Management, 23(3), 1-4.

[20] Chang, S. E. & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458. https://doi.org/10.1108/02635570710734316

[21] Chang, V., Muñoz, V.M. &Ramachandran, M. (2020), 'Emerging applications of internet of things, big data, security, and complexity': special issue on collaboration opportunity for IoTBDS and COMPLEXIS. Computing 102, 1301–1304 (2020).https://doi.org/10.1007/s00607-020-00811-y

[22] Chen, H., & Li, W. (2014, June). Understanding Organization Employee's Information Security Omission Behavior: an Integrated Model of Social norm and Deterrence. In PACIS (p. 280).

[23] Čolaković, A., and Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144 (2018), 17-39.

[24] Dewa, M.T, van der Merwe, A.F and Matope, S. (2018). Digitalisation of shop-floor operations in the south African tool, die, and mould- making industry'. South African Journal of Industrial Engineering, 29(2),153-170.

[25] Diver, S. (2007). Information security policy-a development guide for large and small companies. Sans Institute, 1-37.

[26] El Saghier, N., and Nathan, D. (2013, April).Service quality dimensions and customers' satisfactions of banks in Egypt.In Proceedings of 20th International Business Research Conference. 13.

[27] Elsaadany, A., and Soliman, M. (2017). Experimental Evaluation of Internet of Things in the Educational Environment. International Journal of Engineering Pedagogy (iJEP), 7(3), 50-60.

[28] Emrah, I and Mehmet, B. (2018). 'Internet of Things (IOT): The Most Up-To-Date Challenges, Architectures, Emerging Trends and Potential Opportunities'. International Journal of Computer Applications. 179 (40), 0975 – 8887.

[29] Erceg, A (2019). Information security: threat from employees. JO -Tehničkiglasnik. Pp. 123-128. Vol. 13.DO - 10.31803/tg-20180717222848

[30] Eshan, MRandBinoy, TA. (2018). The Role of Digitalization in Human Resource Management in Star Category Hotels: A Review. Journal of Emerging Technologies and Innovative Research (JETIR), 5(12), 203-211.

[31] Fernández-Caramés, T. M., and Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access.

[32] Fernandes E, Rahmati A, Eykholt K, Prakash A. Internet of things security research: a rehash of old ideas or new intellectual challenges? IEEE Secur Priv. 2017;15(4):79–84

[33] Fosty, V., Eleftheriadou, D., Combes, C., Willemsens, B.,Wauters, P., and Vezbergiene, A. (2013). Doing Business in the Digital Age: The Impact of New ICT Developments in the Global Business Landscape – Europe's Vision and Action Plan to Foster Digital Entrepreneurship, 1–71.

[34] Gallego, B. C., and Drexl, J. (2019). IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework?. IIC-International Review of Intellectual Property and Competition Law, 50(1), 135-156.

[35] Gierlich, M., Volkwein, M., Schüritz, R., Hess, T (2019). SMEs' Approaches for Digitalization in Platform Ecosystems. Twenty-Third Pacific Asia Conference on Information Systems, China 2019.

[36] Gubbi, J., Buyya, B., Marusic, S., Palaniswami, M. (2014). Internet of Things (IOT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29, 1645-1660.

[37] Henriette, E., Feki, M., and Boughzala, I. (2015). The Shape of Digital Transformation: A Systematic Literature review' MCIS 2015 Proceedings. 10.

[38] Hsu, C. L., and Lin, J. C. C. (2018). Exploring Factors Affecting the Adoption of Internet of Things Services. Journal of Computer Information Systems, 58(1), 49-57.

[39] Hussien, M. I., Abd El Aziz, R., &Oatley, G. (2014). Perception and ranking of internet banking service quality from banker perspective in public and private banks in Egypt. International Journal of Research, 1(8).

[40] Hussien, M, I. and Abd El-Aziz, R. (2019), 'System Dynamics Modelling and Simulation for E-Banking: The Egyptian Context'. In Martin Garcia, Juan (Ed.), Modelling the Economy: Money and Finances.Selected Papers on System Dynamics Collection, (pp. 70 - 84). KDP Publishers, ISBN: 9781687003133.

[41] Hussien, M. I. and Abd El Aziz, R. (2016), 'Simulating Banking Service Quality Websites in Egypt: A System Dynamic Approach', In Proceedings of the 28th International Business Information Management Association Conference, 9-10 November 2016, Seville, Spain, 4325-4340, ISBN: 978-0-9860419-8-3.

[42] Hussien, M., I., and Abd El Aziz, R. (2017), 'System Dynamics Modelling and Simulation for E-Banking: The Egyptian Context', IBIMA Business Review Journal, 2017, 1-17. DOI: 10.5171/2017.904520. ISSN: 1947-3788

[43] Jindal, F., Jamar, R., and Churi, P. (2018). Future and challenges of internet of things. International Journal of Computer Science and Information Technology (IJCSIT), 10 (2), 13-25.

[44] Hair, J., Carole L. Hollingsworth, Adriane B. Randolph, Alain Yee Loong Chong, (2017), 'An updated and expanded assessment of PLS-SEM in information systems research', Industrial Management and Data Systems, 117(3), 442-458.

[45] Kandil. O. and Abd El Aziz, R. (2018), 'Evaluating the Supply Chain information flow in Egyptian SMEs using Six Sigma: A Case Study', International Journal of Lean Six Sigma, 9 (4), Emerald, DOI 10.1108/IJLSS-10-2016-0066.

[46] Kandil, O., Abd El Aziz, R., Rosillo, R., and De la Fuente, D. (2019), 'Investigating the Impact of Internet of Things on the Educational Business Process', In Proceedings of the 13th International Conference on Industrial Enginering and Industrial Management, 11-12 July 2019, Gijón, Spain.

[47] Kaushal, P. & Khan, R. (2018). A Review on Information Security. International Journal of Advanced Research in Computer Science and Software Engineering, 8(4), 122-124. https://doi.org/10.23956/ijarcsse.v8i4.646

[48] Khanboubi, F., Boulmakoul, A., and Tabaa, M. (2019). Impact of digital trends using IoT on banking processes. Procedia Computer Science, 151, 77-84.

[49] Kumar, M., Annoo, K., and Mandal, R. K. (2018). The Internet of Things Applications for Challenges and Related Future Technologies and Development. context, 5(1).

[50] Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Parizi, R. M., and Choo, K. K. R. (2018). Fog data analytics: A taxonomy and process model. Journal of Network and Computer Applications.

[51] Lee, S. K., Bae, M., and Kim, H. (2017). Future of IOT networks: A survey. Applied Sciences, 7(10), 1072.

[52] Mathew, N and Nitha, K. (2016), 'Smart Academy an IOT approach: A survey on IOT in education', International Journal of Advanced Research Trends in Engineering and Technology, 3 (2), ISSN 2394-3777 (Print), ISSN 2394-3785 (Online).

[53] Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in security policy development.

[54] MCIT (2019), ICT Indicators in Brief, official report for the Egyptian Ministry of Communication and Information Technology, available at: http://www.mcit.gov.eg/Upcont/Documents/Publications_912020000_ICT_Indicators_in_Brief_November_2019.pdf (accessed January 18, 2020).
[55] McQuitty S, Wolf M (2013) Structural equation modelling: a practical introduction. J Afr Bus 14(1), 58–69.
[56] Narodnenovine. (2007). Zakon o tajnostipodatakaiinformacijskojsigurnosti (in Croatian)
[57] Momani, A. M. (2020). The Unified Theory of Acceptance and Use of Technology: A New Approach in Technology Acceptance. International Journal of Sociotechnology and Knowledge Development (IJSKD), 12(3), 79-98.
[58] Ndung'u, N. S. (2018). Harnessing Africa's digital potential: New tools for a new age.
[59] Neeraj. (2018). Role of Digitalization in Human Resource Management.International Journal of Emerging Technologies and Innovative Research (www.jetir.org). 5(1), 284-288.
[60] Nura, B. and Baharudin, A (2020). Determinants of Users' Intention to Use IoT: A Conceptual Framework. Emerging Trends in Intelligent Computing and Informatics (pp.980-990) DOI: 10.1007/978-3-030-33582-3_92
[61] Omoyiola, B. (2020). Factors affecting IOT adoption. Journal of Computer Engineering (IOSR-JCE), 21(6), 19-24.
[62] Parviainen, P., Tihinen, M., Kääriäinen, J., and Teppola, S. (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. International Journal of information systems and project management, 5(1), 63-77.
[63] Raza, S., Misra, P., He, Z., and Voigt, T. (2017). Building the Internet of Things with bluetooth smart. Ad Hoc Networks, 57, 19-31.
[64] Rose GA, and Rowe S. 2015. Northern cod comeback. Canadian Journal of Fisheries and Aquatic Sciences, 72: 1789–1798. DOI: 10.1139/cjfas-2015-0346.
[65] Rossman, J. (2016). The Amazon Way on IOT: 10 Principles for Every Leader from the World's Leading Internet of Things Strategies", Clyde Hill Publishing.
[66] Roussou, I., Stiakakis, E., Sifaleras, A. (2019), An empirical study on the commercial adoption of digital currencies, Syst E-Bus Manage 17:223–259 (2019). https://doi.org/10.1007/s10257-019-00426-7
[67] Ryan, P. J., and Watson, R. B. (2017). Research Challenges for the Internet of Things: What Role Can OR Play?. Systems, 5(1), 24.
[68] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., and Ande, R. (2018). IoT standardisation: challenges, perspectives and solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (p. 1). ACM.
[69] Schumacher, A., Sihn, W., and Erol, S. (2016), "Automation, digitization and digitalization and their implications for manufacturing processes", Conference: Innovation and Sustainability International Scientific Conference. Sustainable Innovative Solutions 2nd Edition, Bucharest, Romania
[70] Sethi, P., and Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering.
[71] Shang, X., Yin, H., Liu, A., Wang, Y., and Wang, Y. (2020), Secure Green-Oriented Multiuser Scheduling for Wireless-Powered Internet of Things, Special issue of Recent Advances in Security and Privacy Issues for Internet of Things Applications, Wireless Communications and Mobile Computing, Wiley, 1-11. https://doi.org/10.1155/2020/7845107
[71] Singh, P. (2017). Impact of digitalization on small and medium enterprises in India. Indian Journal of Research, 6(4), 468-469.
[72] Strohmeier, S. (2018). Smart HRM–a Delphi study on the application and consequences of the Internet of Things in Human Resource Management. The International Journal of Human Resource Management, 1-30.
[73] Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015). The influence of technology on the future of human resource management. Human Resource Management Review, 25(2), 216–231. https://psycnet.apa.org/doi/10.1016/j.hrmr.2015.01.002
[74] Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., and Catalão, J. (2017). A review of smart cities based on the internet of things concept. Energies, 10(4), 421.

[75] Torchia, M., Shirer, M.,(2019). IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors, International Data Corporation.

[77] Uviase, O., and Kotonya, G. (2018). IOT architectural framework: connection and integration framework for IOT systems. arXiv preprint arXiv:1803.04780.

[78] Venkatesh, A. N. (2017). 'Connecting the Dots: Internet of Things and Human Resource Management'. American International Journal of Research in Humanities, Arts and Social Sciences, 17(1), 21-24

[79] Vankatesh, V., J. Thong, and X. Xu. (2012) "Consumer Acceptance and Use of Information Technology: Extending The Unified Theory of Acceptance and Use of Technology." MIS Quarterly 36 (1): 157-178.

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

[81] Venkatesh, V., Thong, J. Y., &Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. Journal of the association for Information Systems, 17(5), 328-376.

[82] Vivekananth.P. (2016). The Impact of Internet of Things (IOT) in Human Resource Management. IPASJ International Journal of Management (IIJM), 4 (9),1-3.

[83] Wachel, R. "Humanities and Computers," North Am. Rev., pp. 30–32, 1971.

[84] Yadav, P., Mittal, A., and Yadav, H. (2018). IOT: Challenges and Issues in Indian Perspective. 3rd IEEE International Conference on Internet of Things: Smart Innovation and Usages (IOT-SIU 2018), 24-25.

[85] Ziegeldorf, J. H., Morchon, O. G., and Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742.

[86] Internet World Stats, (2019), https://www.internetworldstats.com/stats5.htm

Appendix: Questionnaire Form

Appendix: Questionnaire Form					
A. Answer the following questions:					
1. **Gender**:	O Male	O Female			
2. **Age**:	o 21-24	o 25-34	o 35-44	o 45-54	o 55-64
3.Work experience:					
	O < than 5 years	O 5 to 10 years	O 10 to 15 years	O 15 to 20 years	O > than 20 years
4.Education:					
	O Bachelor's degree	O Master's degree	O Diploma degree	O Doctorate degree	
5. Monthly income:					
	O < than 10,000	O 10,000 to 19,999	O 20,000 to 34,999	O 35,000 to 49,999	O >than 50,000
6. What types of IOT applications is your organisation involved in or planning to be involved in?					
a. Recruitment					
b. Selection					
c. Compensation					
d. Training and Development					
e. Appraisal					
f. Others, please state ---					
7. The greatest challenge to the Internet of Things over the next 5 years is:					
a. Security					
b. Software development					
c. Intention of users					
d. Complex dependencies [such as "Things" taking smart decisions (like humans) in conflicting situations]					
e. Rules and regulations					
f. Networking					
g. Others, please state ---					
8. The greatest risk (threat) on "Things" connected over the Internet:					
a. Hacking					
b. Fraud					
c. Revealing private information					
d. Others, please state ---					

B. Please answer the following statements to indicate your answer on a scale of 1 to 5, where 1 means Strongly Disagree and 5 means Strongly Agree

Questions

9. I have heard about the term "Internet of Things".
10. In my organisation some devices / "Things" are connected together through the Internet.
11. The number of things connected in my organisation has increased over the last 2 yrs.
12. IOT increases the chance of security breaches.
13. It is difficult to assure data security due to the number of devices connected to internet.
14. Information flow in IOT is insecure; as devices may trick users to reveal private data.
15. My organisation manages the risk of devices/" Things" connected to the Internet.
16. My organisation's network can handle all devices/" Things" connected to the Internet.
17. Diversity of devices used will affect the quality and reliability of communication.
18. An open-source software is essential for the compatibility of devices/things connected.
19. The whole setup of an IOT-based organisations may not be expensive.
20. Speed is a critical factor for communication of devices.
21. Complex system/devices is a critical factor for efficiently utilising IOT.
22. Power consumption is a critical factor for efficiently utilising IOT.
23. Cost is a critical factor for utilising IOT.
24. Battery lifetime is a critical factor for utilising IOT.
25. IOT encourages me to use the latest technology
26. I prefer working in an enterprise with IOT technology

27. IOT can improve employee's learning skills
28. IOT can improve employees' learning experience
29. IOT applications such as recording employees' check in and out automatically is interesting.
30. I would not use IOT because of privacy concerns.
31. I prefer mobile activities services at my organisation
32. I believe we are not yet ready for using IOT.
33. IOT can have negative consequence and distractions.
34. Representing human behavior through IOT software is a real challenge.
35. Software developers will be able to model human behavior effectively in future.
36. Devices/" Things" may be required to prioritize conflicting tasks.
37. Devices/" Things" are not smart enough to resolve problems in real time.
38. Real time coordination between devices/" Things" is necessary to avoid wrong actions.
39. Data sent and received by devices/" Things" connected is valid and reliable.
40. Decisions taken from data sent and received is trusted to manage everyday activities
41. Configuring and updating devices/" Things" remotely is essential.
42. Standardization of devices/" Things" is critical for IOT compatibility.
43. The involvement of government in setting IOT security regulations is critical.
44. Utilising standards and protocols such as ISO and IEEE enhance IOT effectiveness.
45. I am aware of IOT security regulations.
46. The announcement of IOT regulations enhances trust among users.
47. The announcement of IOT regulations motivates users, developers and manufacturers.