International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 5293-5308

An Empirical Analysis Of Factors Influencing Iot In Healthcare Environment Applying Tam Model

Dr.B.Sundaravadivazhagan
Professor,
Department of information technology
AL Musanna College of Technology
Musanna
Sultanate of Oman
bsundaravadivazhagan@gmail.com

Dr.B.N.Padmaja Priyadarshini
Managing Director, M/s HomePlanGuru Civil Consultants P Ltd
I Floor No 2 Voltas Colony II Street Nanganallur Chennai
Priya@HomePlanGuru.com

Abstract

IoT also referred as Internet of Things is an inexorablesmart toolwith numerousclaims in diverse fields. HealthCare environment is an important field to adopt IoT.The IoT support innovation of modern health care remote technology with help of the patient to improve the quality of treatment in addition to more convenient and more economical. The study pertains to identify the factors influencing IoTin HealthCare environment and also suggest the solutions via counter measures for the same by application of TAM. The security challenges and issues in IoT health care can be addressed by ensuring confidentiality of the patient data. The study reveals that the challenge lies in motivating patients to adopt the new technology.

Key Words : *HealthCare Environment, IoT, TAM.*

INTRODUCTION

The HealthCare technology is fast growing with pioneering technology ideas. The IoT will bring the powerful changes in hospital industry, such as monitoring patient in remote and offer consultation. The IoT is the spectacle by offering connectivity to physical things through internet and facilitate interaction among themselvesin a remote approach. The trend in the present year (2020) is to witness the rapid growth of IoT devices to an extent of 50 billion. Latest study discloses that IoT has huge potential in the field of healthcare. According to the IoT industry forecasts, IoT healthcare will reach $534.3 billion by 2025.

The important key factor of IoT-Health care technology is to provide quality treatment with minimal cost. The main purpose of IoT-Healthcare technology can be listed as :

- offer support to medical services,
- effective treatment,
- monitoringpatient in remote and health support services to the old age palliative care patients.

The patients' personal data is essential in the diagnosis of diseases and to monitor health conditions.

Overview of IoT healthcare System Process

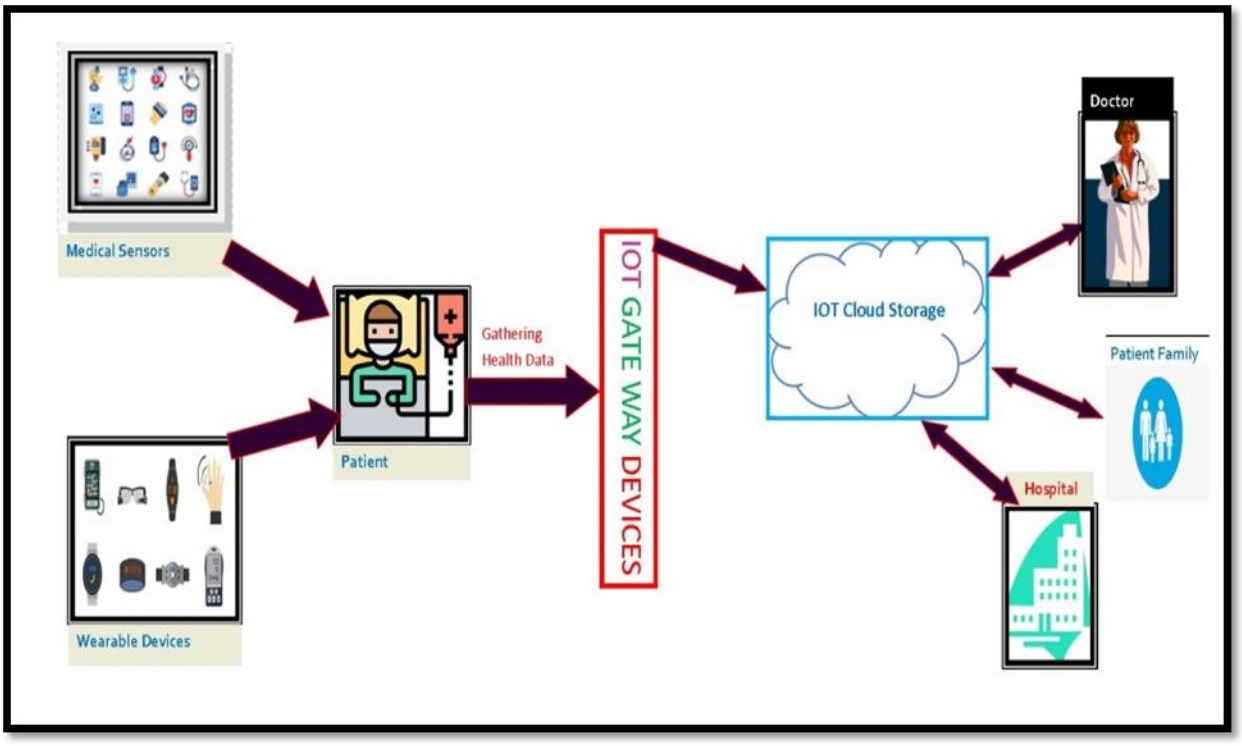

Figure1: IoT Healthcare System model

Figure 1 explains model of IoT healthcare system. The health data are generated from the IoT health care devices such as medical sensors and wearable devices etc.. The data is subsequently transferred toIoT cloud storage through IoT Gateway devices (Zigbee, Wi-Fi, Bluetooth,etc.,). These generated health data analysis is utilized by theconcerned department of hospitals in a meaningful manner tomake timely decisions and give effective treatment. The above model enhances the supporting devices to do efficient communication. The components of the model can be explained as :

- Gateways device support IoT Healthcare:,
- Communication devices support IoT Healthcare:
- Cloud storage support IoT Healthcare

The conceptual study of this paper is to ensure the factors influencing IoT in healthcare environment and the applications of IoT is essential for the same which can be identified as Health Monitoring System model, Emergency Alert monitoring system model, Glucose Level Monitoring Applications, Blood Pressure Monitoring Applications, Heart Based Monitoring Applications, Body Temperature monitoring Applications, Oxygen Saturation Monitoring Applications. The advantages of IoT healthcare applications are given as :Simultaneous reporting and monitoring**,** End-to-end connectivity**, d**ata collection and analysis, Tracking and alerts, Drug Management**.** However, there are principles of security support for standard IoT healthcare applications which is explained in Figure 2.

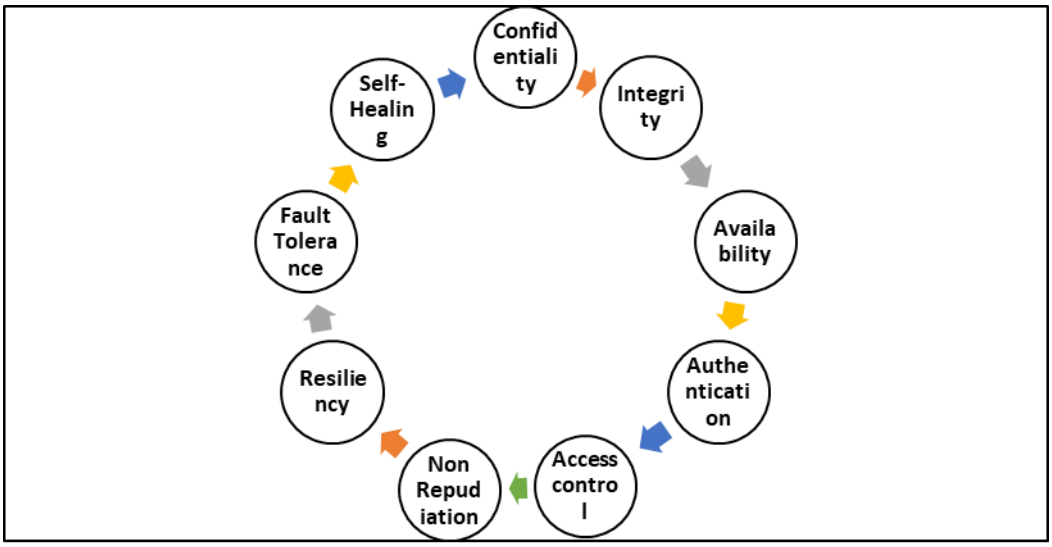

Figure2: General principles of Computer security process

THREATS, VULNERABILITIES AND ATTACKS IN IOT HEALTHCARE APPLICATIONS:

IoT devices in healthcare applications connected devices have their own possible ways for being hacked gaining access in the systems.

a) Gaps are possible in the security when the health care devices connected through IoT in increased number
b) Exploitation of hospital health data and patients' personal data is possible.
c) Patient health data can be exploited for gaining access.

SECURITY COUNTERMEASURES AND MECHANISMS:

The possible counter measures are findings to protect against hacking the IoT Healthcare applications.The Current wirelessnetworking technologies such as Wi-Fi, BLE and ZigBeeand these include different types of medical devices and sensor support intheIoT healthcare environment. These recent technologies provide the security protection which is help to against common threats, vulnerabilities and security attacks. Some of the security mechanisms help to protect patient information from IOT heathcare environment.

a) Cryptography-Encryption Standard Mechanism
b) Light Weight Cryptography
c) Random number generations
d) Hardware devices –Built in Security technologies
e) Intrusion detection Technologies
f) Machine Learning Technologies
g) Block Chain Technologies

REVIEW OF LITERATURE:

In this section deals the review of literature in recent years,many investigation were published toaccentuate the improvement of research activities in the IoT Healthcare environment.

The overview of the literature survey related diagram is shown in Figure 3

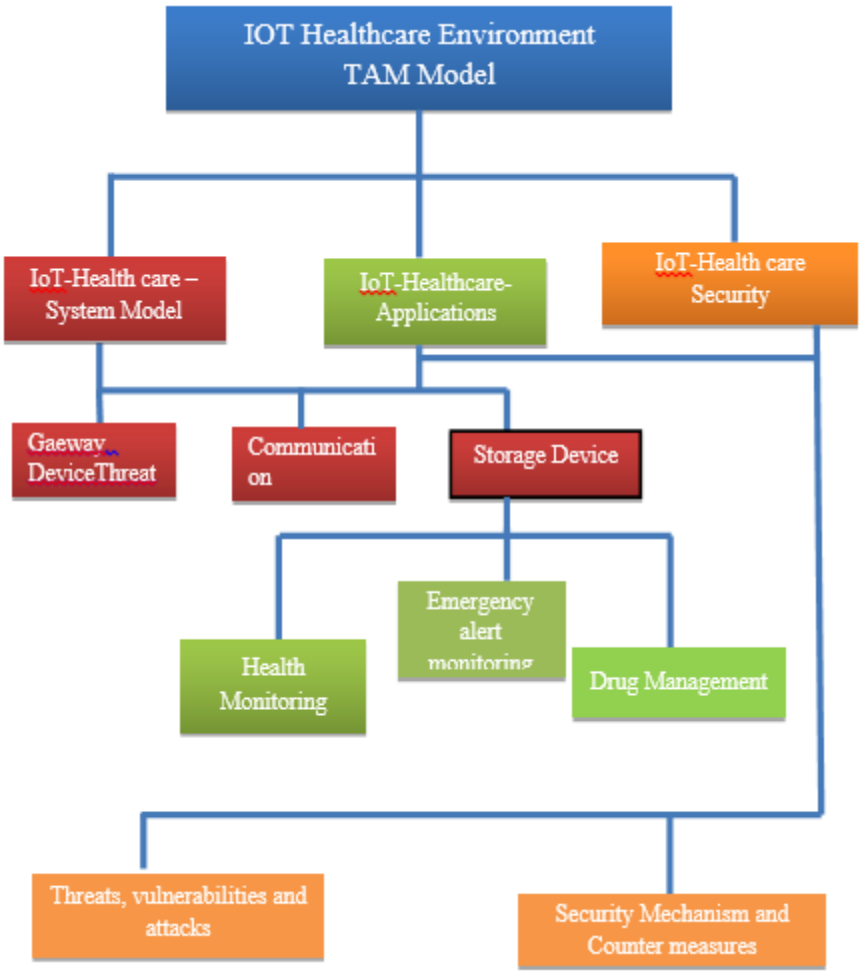

Figure 3: overview of the literature survey

HadiHabibzadeh, et al. (2020) surveyed new technologies which are help to IoT Healthcare Environment. It is also discussed sensing, communication and data analytical technology and issues and challenges in health care internet of things. The survey investigated two main aspects of IoT healthcare communication characteristics such as connectivity and data aggregation. The majority of implementations in IoT healthcare applications either BLE or Zigbee and also summarized alongwithsome common issues and challenges such as ingle-hub, no-multicasting, rerouting delay, static power management and poor coexistence. The survey focused on data analytical and inference. In recent years, much more health data are generated from IoT Health care devices and some of the data analytics and inference algorithms, which are now used in variety of health care.IoT applications for prediction of future health events, early detection of diseases, cost reduction and clinical decision support. The study covered the issues arising due to the availability of the data that can be used in the algorithm.

Francesca Meneghello, et al. (2019) investigated impact of the security challenges and issues and to discuss some possible counter measures. This survey summarized the some of the recent possible of the security attacks againstthat can target in the IoTcommunication layers such as edge layer, middleware layer, application layer. In this edge layer one of the main threats at this level is represented by the side channel attacks.The application layer attacked target the integrity, there can also be attacks on the authentication credentials. The survey discussed the general security mechanism and challenges in the IoTapplications and security of standard IoT communication technology. The standard encryption, lightweight encryption and secure hardware mechanisms which is to support IoT healthcare environment.In addition this investigation focused on the security mechanisms implemented by some of the communication technologies used in the IoT domain, namely ZigBee, BLE, 6LoWPAN, and LoRaWAN. Furthermore,review of security vulnerabilities and attacks of these technologies were found in the literature.

MeshariAlanazi, et.al. (2019) attempted to develop an extended theoretical model and test it empirically to determine the acceptance of IoT services for healthcare sector in the Kingdom of Saudi Arabia using the Technology Acceptance Model (TAM).The study was developed to investigate the adoption of a new technology, where the Technology Acceptance Model (TAM) is utilized and the quantitative approach is employed and finally proposed novel model that extends the TAM to include another four factors Perceived Connectedness (PCD), Perceived Cost (PC), Perceived Convenience (PCV), and Privacy Concerns (PCO) and to test the relationship among the factors in the proposed model.

Muhammad MahtabAlamet.al. (2018) focused on development ofIoThealthcare end-to-end solution for each application and discovers the communication technologies which is to support overall communication. The survey emphasised the current IoT technology of healthcare applications having some of the features such as remotehealthmonitoringtovideoconsultancy with physician, prediction of diseasesand suitable treatment. The IoT health sensors help in analysing, processing and transmitting health-related data.Furthermore, most of the proposed survey identified long-range communications satisfy the parameters such as, reduced transmission time and higher reliability. Even though these risks are high for the IoT Health care applications for the following reason, increase in number of IoT devices connected to the network, the vulnerability enables the attacker to hack the applications and collect the patient personal health data which is more risky. This survey presented data analytics which is important forIoT healthcare applications.

Amine Rghioui et.al. (2018) delivered an overview of IoT healthcare, current trends and future developments of healthcare systems. This paper discussed analysis of the IoT technologies and their applications and discussed architecture and protocol in IoT healthcare domain. The author proposed discovering the association with the IoT and other developing tools such as wireless sensor networks, RFID technology, and cloud computing.In addition, the study analysed some of the challenges in IoT Healthcare environment such as Adherence monitoring,Limited and prospective time and Integration of multiple devices and protocol.Another challenge is the security challenge, which involves managing credentials and controlling access to patient requests and confidential information. The paper discussedIoT health care applications that are designed to give support to patient and doctors to respond quickly in emergencies and to track the status of a patient. The IoT applications can be found in home monitoring especially for elderly people with special needs or chronic illnesses such as diabetes, congestive heart failure. etc.,

CansuEken, et.al. (2016) discussed overview of IoT healthcare systems and applications, security and privacy challenges and investigate the security threats in different layers of architecture in the loT, and helps to provide security and privacy. The IoT devices collect healthcare data in order to support the healthcare applications. Therefore, security and privacy is important for healthcare systems. This article

focused the IoT devices are exposed by many security vulnerabilities. The energy consuming is an important problem for wearable devices. Because wearable devices they collect healthcare data from patient body continuously. The battery backup energy is not enough to collect and send health data to IoT healthcare applications. The patient health data are collected from IoT sensor devices. These devices gather data by remote access mechanisms which have some challenging about privacy and security.The study reveals trust management is important for IoT devices and applications due to provide security and privacy of data.Denial-of-service attacks (DoS) dangerous attacks for IoT applications because the denied services to the devices, it may lead to big security issues. In addition the paper focused the security counter measures in IoT health care applications. The Access management protects the patient health data from attackers as per the study.

Year	Contribution	Issues
2020	Survey the sensing, communication and data analytical technology and issues and challenges in IOT Healthcare environment.	Some of the common issues are low accuracy, invasive, privacy concerns and noise sensitivity, single-hub, no-multicasting, rerouting delay, static power management and poor coexistence and availability of data.
2019	In this investigation impact of the security challenges and issues and to discuss some possible counter measures.	The attackers use the security vulnerabilities, some of the attack in IoT device attacks are side channel attacks, snooping, and un authorized access, man in the middle attack, spoofing, reply and redirect. and mention some of the mechanisms standard encryption, lightweight encryption and secure hardware.
2019	This study aimed to discuss mobile computing contributions of IoT applications in healthcare, with regard to privacy and security in health IoT devices	Some of the challenges are discussed data management,privacy and security and device level energy Issues.
2018	This survey focuses on the developing IoT healthcare end-to-end solution, security and privacy in IoT healthcare technology, data analytics.	The more number of IoT devices connected to the network is the major vulnerabilities in IoT healthcare applications and the most important challenge of data analytics for future healthcare system.
2018	This article delivers an overview of IoT healthcare, current trends and future developments of healthcare systems.	some of the challenges in IoT Healthcare environment such as Adherence monitoring,Limited and prospective time and Integration of multiple devices and protocol. Another challenge is the security challenge, which involves managing credentials and controlling access to patient requests and confidential information.
2017	The aim of this study is to investigate main factors affecting individuals' intention to adopt internet of things (IoT) products in healthcare	Privacy issue is an important context in adoption of or continuation to use a technology, cost is simply defined as the money required to acquire something, and here refers to the money to be paid by consumers for IoT health products
2016	This research paper discussed overview of IoT healthcare systems and applications, security and	The following issues are energy optimization, security and privacy ,trust management,

	privacy challenges and investigate the security threats in different layers of architecture in the loT, and helps to provide security and privacy	Denial of service attack,
2015	This survey discussed in IoT based health care technologies, network architectures, IoT healthcare applications, different IoT security and privacy features, threats, and attack taxonomies from the health care perspective.	Challenges For Secure IoT Healthcare application services are includeComputational Limitations,Memory Limitations,Energy Limitations,Mobility,Scalability, The Multiplicity Of Devices,A Dynamic Network Topology,Dynamic Security Updates,Tamper-Resistant Packages.

Table 1 - List of contributions in IoT referring healthcare environment.

RESEARCH GAP

Previous studies have discussed aboutIoTbased health care environment with TAM model.Several authors discussed various standard system model, IoT health care applications and IoT health care security which is used to overcome the challenges and issues of various factors in IoT healthcare environment. However, there are no specific studies related to factors influencing IoT and thecounter measures of the IoT applications.

OBJECTIVES OF THE STUDY :

1. To study the socio demographic profile of the respondents of the study
2. To find out the variousinfluencing factors influencing IOT healthcare
3. To study the counter measures of IoT applications in healthcare

RESEARCH METHODOLOGY:

Population of the study: The respondents were selected from various cities who have been involved in IoT in healthcare.

Method of data collection: Survey - Convenience sampling method

Tools for data collection: A structured questionnaire was adopted to collect the data from the respondents.

Sample Size: 76 respondents involved in IoT

Types of data: Primary data questionnaire through google forms

Scaling technique: 5 Point Likert Scale.

STATISTICAL TOOLS USED FOR THE STUDY:

1. Percentage analysis& Descriptive Statistics
2. t - Test& One wayANOVA

LIMITATIONS OF THE STUDY:

Several factors influence IoT in heathcare sector. In this context only few factors taken for research. Moreover the sample size is very less to be generalized..

ANALYSIS AND INTERPRETATION

Data were collected from 76 respondents involved in IoT in healthcare. Demographic profile of the respondents is studied vide frequency distribution and descriptive statistics.

TABLE 2

Socio-Demographic Variables	Frequency	Percentage
Age		
Upto 35 years	16	21
35-45 years	52	69
Atleast 45 years	8	10
Gender		
Male	54	71
Female	22	29
Educational Qualification		
UG	3	4
PG	45	59
Professional	2	3
Others	26	34
Profession		
Academician	4	5
Medical Doctor	52	69
Government	3	4
Civilian	1	1
IT Professional	13	17
Business	3	4

Source: Computed data

1. Most of the respondents (69%) belonged to the age group 35-45.
2. The survey had majority (71%) as males.
3. Majority of the respondents (59%) possess PG level of educational qualifications
4. 69% of the respondents were medical doctors with respect to profession.

DESCRIPTIVE STATISTICS

Descriptive statistics of the variables related to IoT are evaluated in the present study. Eleven variablesrelated to IoTare identified along with mean and S.D and communalities are exhibited in the table 3.

Table 3

Variables	Mean	S D
Internet Usage Experience	4.75	0.436
Internet Connectivity	4.42	0.771

IoT Health Care –Applications -Awareness	4.08	0.796
IoT Health Care –Usage of Smart Devices	4.11	0.810
Mobile Sensors Usage	4.00	0.924
IoT Health Care- Mobile Health Sensors Applications usage	3.93	0.884
Familiarity with IoT Health Care Sensors	3.84	0.939
IoT Health Care- Wearable devices health Sensors Usage	3.86	0.890

Source: Computed data

PERCENTAGE ANALYSIS

The overall perception of various factors in IoT Healthcare Development is explained vide Table 4.

Table 4

Various Factors in IoT Healthcare Development	**SA**	**A**	**N**	**DA**	**SDA**
	f (%)	**f (%)**	**f (%)**	**f (%)**	**f (%)**
Number of IoT Health care devices to connect internet-Chance to exploit system	26(35)	35(46)	10(12)	4(5)	1(2)
Hospital Security System-Possible to exploit Patient Health information	23(30)	32(43)	18(23)	2(3)	1(1)
Power Management-Energy issues in IoT Health care Devices	26(34)	24(32)	16(20)	10(14)	-
Unauthorized Access	20(26)	27(35)	20(26)	7(10)	2(3)
Default password	25(33)	32(42)	14(18)	5(7)	-
Medical Health Data-Security and Privacy	28(37)	24(32)	20(26)	4(5)	-
Medical Health Data- Confidentiality, Integrity, Availability and Poor authentication	21(28)	24(32)	26(34)	5(6)	-
Attack –Man in the middle attack, Denial of service attack.	33(43)	30(40)	12(16)	1(1)	-

Source: Computed data

The overall perception of counter measures of IoT Healthcare Development is explained in Table 4**.**

t - Test :

Null Hypothesis H_{01A}: Viewed upon the gender of the respondents, there is no influence on the perception of the factors influencing IoT Healthcare Development.

Table 5 Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
FACTORS	Male	54	32.9815	5.17793	.70463
	Female	22	28.5909	5.97343	1.27354

Table 6

FACTORS	t-test for Equality of Means	T	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
	Equal variances assumed	3.205	74	.215	4.39057	1.36975
	Equal variances not assumed	3.017	34.542	.215	4.39057	1.45547

Since P Value > 0.05, null hypothesis is accepted.

Inference : Viewed upon the gender of the respondents, there is no influence on the perception of the factors influencing IoT Healthcare Development.

One way ANOVA :

Null Hypothesis H_{01B}: Viewed upon the age of the respondents, there is no influence on the perception of the factors influencing IoT Healthcare Development.

Table 7 ANOVA					
FACTORS					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	28.959	2	14.479	.433	.000
Within Groups	2442.673	73	33.461		
Total	2471.632	75			

Since P value < 0.05, null hypothesis is rejected.

Inference : Viewed upon the age of the respondents, there is influence on the perception of the factors influencing IoT Healthcare Development.

Null Hypothesis H_{01c}: Viewed upon the profession of the respondents, there is no influence on the perception of the factors influencingIoT Healthcare Development.

Table 8 ANOVA					
FACTORS					
	Sum of Squares	Df	Mean Square	F	Sig.

Between Groups	81.394	5	16.279	.477	.002
Within Groups	2390.237	70	34.146		
Total	2471.632	75			

Since P value < 0.05, null hypothesis shall be rejected.
Inference : Viewed upon the profession of the respondents, there is influence on the perception of the factors influencing IoT Healthcare Development.

Null Hypothesis H_{01D}: Variables of IoT Health Care do not influence the factors adopted by IoT Healthcare Development.

Table 9 ANOVA					
FACTORS					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1597.454	16	99.841	6.738	.000
Within Groups	874.178	59	14.817		
Total	2471.632	75			

INFERENCE :

Variables of IoT Health Care influence the perception of the factors ofIoT Healthcare Development.

Table 10

Counter Measures of IoT Applications in Health Care	**SA**	**A**	**N**	**DA**	**SDA**
	f (%)	**f (%)**	**f (%)**	**f (%)**	**f (%)**
Hardware devices –Built in Security technologies	31	31	14	-	-
Standard encryption Technologies with Random number Generation	32(42)	31(41)	13(17)	-	-
Cryptography-Encryption Standard Mechanism	24(31)	37(49)	14(18)	1(1)	-
Light Weight Cryptography- Encryption Standard Mechanism	31(41)	32(42)	13(17)	-	-
Intrusion detection Technologies	30(40)	35(46)	11(14)	-	-
Machine Learning Applications	22(29)	35(46)	14(18)	3(4)	2(3)
Block Chain Technologies	26 (34)	24(32)	16(21)	10(14)	-

Source: Computed data

t- TEST :

Null Hypothesis H_{02A}: Viewed upon the gender of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development.

Table 11 Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
COUNTER_MEASURES	Male	54	29.7778	4.05000	.55114
	Female	22	26.6818	4.61247	.98338

Table 12

COUNTER MEASURES	t-test for Equality of Means	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
	Equal variances assumed	2.902	74	.102	3.09596	1.06667
	Equal variances not assumed	2.746	34.900	.345	3.09596	1.12729

Since P value > 0.05, null hypothesis shall be accepted.

Inference : Viewed upon the gender of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development.

One way ANOVA :

Null Hypothesis H_{02B}: Viewed upon the age of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development.

Table 13 ANOVA

COUNTER_MEASURES					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	33.415	2	16.707	.851	.001
Within Groups	1432.519	73	19.624		
Total	1465.934	75			

Since P value < 0.05, reject null hypothesis.

Inference : Viewed upon the age of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development**.**

Null Hypothesis H_{02C}: Viewed upon the profession of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development.

Table 14 ANOVA

COUNTER_MEASURES				

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	28.293	5	5.659	.276	.000
Within Groups	1437.641	70	20.538		
Total	1465.934	75			

Since P value < 0.05, reject null hypothesis.

Inference : Viewed upon the profession of the respondents, there is influence on the perception of the counter measures influencing IoT Healthcare Development.

Null Hypothesis H_{01D}: Variables of IoT Health Care do not influence the perception of the counter measuresadopted by IoT Healthcare Development..

Table 15 ANOVA

COUNTER_MEASURES					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	953.265	16	59.579	6.857	.000
Within Groups	512.669	59	8.689		
Total	1465.934	75			

Since P value < 0.05, null hypothesis is rejected.

Inference : Variables of IoT Health Care influence the perception of the counter measures adopted byIoT Healthcare Development.

FINDINGS OF THE STUDY :

1. Most of the respondents (69%) belonged to the age group 35-45.
2. The survey had majority (71%) as males.
3. Majority of the respondents (59%) possess PG level of educational qualifications
4. 69% of the respondents were medical doctors with respect to profession.
5. Viewed upon the gender of the respondents, there is no influence on the perception of the factors influencing IoT Healthcare Development.
6. Viewed upon the age of the respondents, there is no influence on the perception of thecountermeasures influencing IoT Healthcare Development.
7. Viewed upon the profession of the respondents, there is influence on the perception of the counter measures influencing IoT Healthcare Development.
8. Variables of IoT Health Care influence the perception of the factors of IoT Healthcare Development.
9. Viewed upon the gender of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development.

10. Viewed upon the age of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development**.**

11. Viewed upon the age of the respondents, there is no influence on the perception of the counter measures influencing IoT Healthcare Development**.**

12. Variables of IoT Health Care influence the perception of the counter measures adopted by IoT Healthcare Development.

CONCLUDING REMARKS :

The study contributed in the identification of factors influencing IoT in HeathCare Environment and also suggested the counter measures towards IoT in HealthCare Environment. The variables of IoT in Health Care Environment were listed as : Internet usage experience, Internet connectivity, IoT health care – Applications -Awareness, IoT HealthCare –Usage of smart devices, Familiarity with IoT HealthCare sensors, IoT HealthCare- Wearable devices health sensors usage, IoT HealthCare- Mobile Health Sensors Applications usage&Mobile Sensors Usage. The various factors affecting IoT in HealthCare Environment according to the study were enlisted as : number of IoT HealthCare devices to connect internet-chance to exploit system, Hospital security system-possiblility to exploit patient health information, Power management-energy issues in IoT HealthCare devices, Unauthorized access, Default password, Medical health data-security and privacy, Medical health data-confidentiality, integrity, Availability and poor authentication. The counter measures suggested to improve the factors influencing IoT in HealthCare Environment were identified as: Hardware devices –Built in Security technologies, Standard encryption Technologies with Random number Generation, Cryptography-Encryption Standard Mechanism, Light Weight Cryptography- Encryption Standard Mechanism, Intrusion detection Technologies, Machine Learning Applications&Block Chain Technologies.

REFERENCES

1. AdemKarahoca, DilekKarahoca, Merve Aksöz, Examining intention to adopt to internet of things in healthcare technology products,Kybernetes, https://doi.org/10.1108/K-02-2017-0045 ,2017.
2. Amine Rghioui, AbdelmajidOumnad, Challenges and Opportunities of Internet of Things in Healthcare,International Journal of Electrical and Computer Engineering (IJECE) Vol. 8, No. 5, October 2018, pp. 2753~2761 ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp2753-2761.
3. Anil Chacko1,ThaierHayajneh1,SecurityandPrivacyIssueswithIoTinHealthcare,EAI Endorsed Transactions on Pervasive Health and Technology ,02-2018 -07-2018,volume 4,issues 14,e2.
4. BrijeshSivathanu, Adoption of internet of things (IOT) based wearables for healthcare of older adults a behavioural reasoning theory (BRT) approach, journal of Enabling Technologies,VOL. 12 NO. 4 2018, pp. 169-185,© Emerald Publishing Limited, ISSN 2398-6263.
5. CansuEken, HanımEken, Security Threats and Recommendation in IoT Healthcare,DOI: 10.3384/ecp17142369, Proceedings of the 9th EUROSIM & the 57th SIMS,2016.
6. Coetzee.L, Fksteen.J, "The internet of things – promise for the future? An introduction", IST-Africa Conference Proceedings, 2011.
7. D. M. West, ''How 5G technology enables the health Internet of Things,'' Center Technol. Innov. Brookings, Washington, DC, USA, Tech. Rep., 2016, pp. 1–20. [Online]. Available: https://www.brookings. edu/research/how-5g-technology-enables-the-health-internet-of-things/

8. Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese , IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices and Andrea Zanella , IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 5, OCTOBER 2019.
9. H. Lin, W. Xu, N. Guan, D. Ji, Y. Wei, and W. Yi, "Noninvasive and continuous blood pressure monitoring using wearable body sensor networks," IEEE Intell. Syst., vol. 30, no. 6, pp. 38–48, Nov./Dec. 2015.
10. Hadi,Omid Rajabi , Gaurav "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective",IEEE Internet Of Things Journal, Vol. 7, No. 1, January 2020.
11. Imran Makhdoom, Mehran Abolhasan , Justin Lipman , Ren Ping Liu,Wei Ni,Anatomy of Threats to the Internet of Things,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 2, SECOND QUARTER 2019.
12. M. Aazam, I. Khan, A. A. Alsaffar, E.-N.Huh, "Cloud of internet integrating Internet of things and cloud computing and the issues involved", 11th International Conference on Applied Sciences and Technology (IBCAST), 2014.
13. M. Kachuee, M. M. Kiani, H. Mohammadzade, and M. Shabany, "Cuffless blood pressure estimation algorithms for continuous healthcare monitoring," IEEE Trans. Biomed. Eng., vol. 64, no. 4, pp. 859–869, Apr. 2017.
14. M.M.DhanvijayandS.C.Patil,"InternetofThings:asurvey of enabling technologies in healthcare and its applications," Computer Networks, vol. 153, pp. 113–131, 2019.
15. MeshariAlanazi and Ben Soh ,Internet of Things for Healthcare Purposes: Extending the Technology Acceptance Model for Saudi Arabia Patients,IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.2, February 2019.
16. Muhammad,Elyes Ben Hamida,"Surveying Wearable Human Assistive Technology for Life and Safety Critical Applications: Standards, Challenges and Opportunities," Sensors 2014, 14, 9153-9209; doi:10.3390/s140509153.
17. Muhammad,Hasan, Muhidul,Tamas,Alar,Yannick,"A survey on the roles of communication Technologies in IoT-Based Personalized Healthcare Applications,"IEEE Access,2018.
18. Nambiar,A.R.,Reddy,N.andDutta,D.(2017), "Connectedhealth:opportunitiesandchallenges",IEEE InternationalConferenceonBigData,IEEE,Boston,MA,pp.1658-1662.
19. P. Fremantle and P. Scott, "A survey of secure middleware for the Internet of Things," Peer J. Comput. Sci., vol. 3, p. e114, May 2017.
20. R. H. Weber, "Internet of Things—New security and privacy challenges," Comput. Law Security Rev., vol. 26, no. 1, pp. 23–30, Jan. 2010.
21. R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, ''The potential of Internet of m-health Things 'm-IoT' for non-invasive glucose level sensing,'' in Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC), Aug./Sep. 2011, pp. 5264–5266.
22. Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Sherali Zeadally ,Lattice based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions, October 2018,DOI: 10.1109/JIOT.2018.2878707
23. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S.Kwak, "The Internet of Things for health care: a comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.
24. Shah ,Yasir , Naeem Ivan "Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review",Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 5931315, 20 pages.
25. Sherali, Farhan, Zubair, Ahmed, "Smart Healthcare Challenges and Potential solutions using Internet of Things(IoT) and Big data analytics, "PSU Research Review, Emerald Publishing limited,2019.
26. SumitMajumder, M. Jamal Deen," Smartphone Sensors for Health Monitoring and Diagnosis,"Sensors (Basel). 2019 May; 19(9): 2164.

27. T. M. Seeberg et al., "A novel method for continuous, noninvasive, cuff-less measurement of blood pressure: Evaluation in patients with nonalcoholic fatty liver disease," IEEE Trans. Biomed. Eng., vol. 64, no. 7, pp. 1469–1478, Jul. 2017.
28. Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The Internet of Things in healthcare: an overview," Journal of Industrial Information Integration, vol. 1, pp. 3–13, 2016.
29. Yu-Sheng Kao, KazumitsuNawata and Chi-Yo Huang, An Exploration and Confirmation of the Factors Influencing Adoption of IoT-Based Wearable Fitness Trackers,International Journal of Environmental Research and Public Health 2019, 16, 3227; doi:10.3390/ijerph16183227
30. Zeadally,S.andBello,O.(2019),"Harnessingthepowerofinternetofthingsbasedconnectivitytoimprove healthcare",InternetofThings,p.100074,availableat:https://doi.org/10.1016/j.iot.2019.100074

WEBSITES:

31. https://ukdiss.com/examples/iot-healthcare-applications.php
32. https://iotbusinessnews.com/2020/03/25/05014-how-to-apply-iot-in-healthcare-best-approaches-and-use-cases/
33. https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html
34. https://econsultancy.com/internet-of-things-healthcare/
35. https://www.iotforall.com/top-digital-health-solutions/
36. https://www.mdpi.com/journal/ijerph