STAKEHOLDERS' PERSPECTIVES ON WEARABLE INTERNET OF MEDICAL THINGS PRIVACY AND SECURITY

SRAIDI Najla

Abdelmalek Essaadi University, National School of Management-Tangier, Economics and Risk Management (EMR), Morocco

najlasraidi20@gmail.com

ABSTRACT

The Internet of Medical Things (IoMT) is, in fact, a fast-developing healthcare technology that has a great deal of room for improvement in terms of security. Like any other device that is linked to the internet, IoMT is susceptible to security flaws. These breaches have the potential to have an influence not just on the operation of the device, but also on the security and privacy of the data (S&P). The fallout from these violations may have potentially catastrophic and even life-threatening effects. A stakeholder-centric approach was used in the technique that was developed, with the goal of increasing the level of security of transportable IoMT devices. The suggested technique to measure the level of security present inside wearable IoMT's is based on a combination of S&P characteristics that have been defined for such devices. Second, a technique was developed for measuring the level of security included inside such devices. At the end of the presentation, a case study was given to show how the conceptual framework may be used to the grading of Wearable IoMT's with regard to features of S&P. The purpose of this paper is to assist hesitant consumers in choosing an IoMT device that is secure, to encourage healthy competition among makers of IoMT devices, and to ultimately raise the bar for the safety of mobile IoMT devices.

Keywords : IoMT, Wearable Devices, Sensors, Healthcare.

1. INTRODUCTION

The development of new medical technologies fundamentally altered the nature of public healthcare. We no longer need to make frequent trips to the hospital since we could track our own health. Even though this fundamental change is very much welcomed, we must take a step back in order to evaluate the security of such gadgets. Both the security and the privacy of these devices are compromised [1]. Whenever it comes to the safety of medical equipment, the repercussions are serious since the successful functioning of these devices is essential to the survival of a significant number of patients. Because of this, the importance of ensuring patient safety cannot be overstated.

The term "wearable Internet of medical things" refers to intelligent electronic devices that may be worn on the body to enhance the health of patients. These devices can communicate with one another through the Internet [2]. These gadgets are able to monitor almost everything, including the user's physical exercise, temp, sugar levels, sleep, and heart rate, among other things. These electronic gizmos may be purchased in several formats, such as smart armbands, watches, eyeglasses, belts, necklaces, and patches, amongst others [3].

Wearable technology often includes components such as sensors, memories, solar cells, and batteries. They help in the process of data gathering, presentation, and wireless communication of the data that has been acquired [4]. These gadgets may monitor the health state of patients or users and communicate the information directly to doctors, which eliminates the need for a physical visit to the doctor [5].

1.1 Problem Definition

Use of wearable Internet of Medical Things devices is growing year after year. By 2022, the global wearable medical device market is projected to be valued $9.4 billion. Despite all of the technological advances in portable Internet of Medical Things devices, the S&P of these devices is frequently overlooked by both users and manufacturers [6]. Customers looking for wearable Internet of Medical Things devices frequently focus on the design, price, and performance of these devices [7]. Customers are unable to select or rating such devices in terms of data security [8]. Furthermore, stakeholders have different goals and risk tolerance The number of patients who make use of Internet of Medical Things (IoMT) wearable devices continues to rise [9]. It is anticipated that the worldwide market for wearable medical devices would be worth $9.4 billion by the year 2022[10]. The S&P of portable Internet of Medical

Devices devices is commonly disregarded by both the users of these devices and the makers of these devices, despite the many technical advancements that have been made in these devices [11]. Customers that are seeking for wearable Internet of Medical Things gadgets often concentrate on the device's design, pricing, and performance while making their purchasing decisions [12]. Consumers are still unable to pick or rate such gadgets based on how securely their data is stored [13]. In addition, different stakeholders have various objectives and levels of tolerance for risk [14].

1.2 Proposed Solution

Users who are apprehensive about acquiring a smart IoMT (Internet of medical things) device that is more secure might get assistance from this initiative [15]. Additionally, this effort encourages a healthier level of competition among makers of wearable IoMT devices [16]. In addition, this initiative contributes to the enhancement of the safety measures taken by wearable Internet of Things devices [17], [18].

The purpose of this research is to provide hesitating users with guidance on how to choose a trustworthy wearable IoMT device regarding the safety of their data [19]. This research offers the user assistance in picking a gadget with a higher level of safety.

2. LITERATURE REVIEW

Security and privacy concerns about Internet of Things devices the article "Privacy and Security Issues in IOT" provides an in-depth explanation of the privacy and security concerns around Internet of Things devices [20]. Authentication , identifying data, and the diversity of IoT devices are said to be the primary threats to users' privacy and safety posed by the Internet of Things (IoT) [21], [22]. Connectivity, sustainability, morality communication systems, commercial structures, and monitoring are among some of the most significant difficulties posed by IoT devices [23]. This article addresses the problems of privacy and safety that are connected to Internet of Things (IoT) devices. Using a five-dimensional model, the authors of this study investigated the potential risks to users' privacy presented by the model they suggested [24]. The five-dimensional model for privacy consists of the following dimensions: identity privacy, inquiry privacy, personal privacy, footprints privacy, and owner privacy. In depth analysis of both the big picture and the historical context of IoT systems is provided in

this study [25]. This article provided an explanation of the IOT protocol stack and the applications of IOT in a variety of sectors including medical applications, intelligent community security systems, and smart homes [26]. Following a discussion of the Internet of Things and the many software packages associated with it, the writers moved on to a discussion of the Internet of Things' privacy and security concerns [27]. Concerns about the security of the Internet of Things involve not just front-end sensors but also hardware, networking, and back-end information technology systems [28]. Concerns related to privacy in the IoT include the privacy of devices, the privacy of communications, and the privacy of processing [29], [30].

IOT, risks to IOT security, as well as several unresolved concerns in the IOT sector, are all topics that are covered in this study [31]. In this article, the topic of security requirements for today's Internet of Things technology is also discussed. In this article, the challenges that are brought about by IoT devices are discussed [32]. The writers also covered the three layers upon layers that make up IOT, which have been the using the, the transportation layer, and the application layer, in addition to the security challenges that are faced by each layer individually [33]. In addition, cross-layer heterogeneous integration and security challenges, as well as prospective solutions, were investigated and discussed in this study [34]. There are four distinct parts to a piece of writing that has the title "Survey on Privacy and Security in the Internet of Things." In the first part of the article, the writers discussed both the limitations of IoT devices and the potential remedies to those limitations [35]. Those participants in the second phase who concentrated only on the classification of IOT attacks [36]. In the third part of the breakdown, they detailed the processes as well as the architectural style that would be used for authentication and encryption. In the concluding portions, the authors analyzed security concerns present in a number of different levels of IOT [5], [37], [38].

The research article titled "Review on Privacy and Security Issues on the Internet of Things" focused its attention on typical flaws associated with the Internet of Things, such as Distributed Denial of Service (DDOS) assaults and data integrity attacks such data alteration attacks [39]. The following topics are covered in this article: web interface security vulnerabilities; device connections; spamming; data storage concerns; internet of things (IoT) network-related issues; cloud connectivity considerations; and internet of things (IoT) assaults [40]. The article "Security for the Internet of Things: A Questionnaire of Existing Protocols

and Open Research Issues" investigates the protocols and procedures that are already in use to secure Internet of Things communications [41].

In addition, the authors covered known methods for satisfying basic security needs for IoT communications [42]. "This article gives an outline to Production IoT systems, and also the associated privacy and security challenges, as well as an outlook on potential solutions toward a holistic security structure for Industrial IoT systems [43]." This document also includes a listing of the qualities that raise the danger vectors in the internet of things, as well as an explanation of the attacks that target the internet of things [44]. This research does not focus on medical IOT devices, despite the fact that it discusses concerns about privacy and security in relation to the internet of things. The issues around data protection and privacy in IoT technology are the primary focus of this article. This article provides a detailed demonstration of the threats that may occur in IoT devices [45]. The authors categorized the assaults as low, medium, high, and very high in terms of their severity [46]. They also examined the nature and behavior of the assaults, in addition to various countermeasures that may be taken against them [47]. Given the potential dangers posed by Internet of Things (IoT) devices, the researchers also proposed that security methods be included into these devices [48].

Internet of Medical Things (IOMT): The Internet of Medical Things (IOMT) refers to the process of connecting various things to various individuals inside a healthcare facility or across the health system in order to aggregate and analyze information in order to derive IOT actionable insights [49], [50]. In healthcare, the most common use cases rational connection people, consumers, clinicians, and caregivers [51]. Numerous connected health projects have been piloted by healthcare organizations, with the primary goal of increasing consumer engagement [52]. The ability to connect with consumers but also patients but rather affect their actions will allow people to make healthier choices, resulting in better outcomes as well as lower healthcare costs. Monitoring consumers' vital signs and activity, as well as hold them to account for healthcare decisions, will help drive compliance even further [53]. To control healthcare costs, there is a growing emphasis on improving population health around the world. A greater emphasis on consumer engagement and creative technology to integrating IOT-based health care into innovative care delivery I s promoting the use of connected medical technologies.

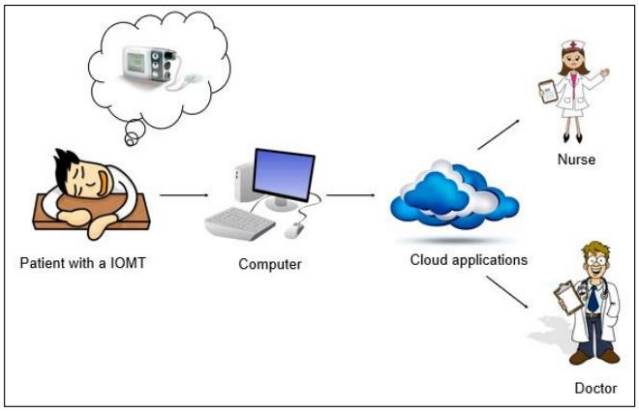


Figure 1: Internet of medical things architecture

Security and privacy issues with the Internet of Medical Things (IOMT): Security, compliance, and product development expenses are the three most pressing issues for businesses and the medical industry in 2017. The signal between both the pulse generator and the programmer, as well as pacemakers and insulin pumps, are all at danger. To put it simply, they might be deadly. There are around 8600 security issues found in pacemakers, which are used to keep people's hearts beating. A guy called Jerome Radcliffe was discovered hacking into and disabling an insulin pump linked to his abdomen at the "Black Hat Technical Security Conference" in Las Vegas in August 2011. As part of an insulin delivery system meant to keep Radcliffe alive by monitoring and maintaining his blood glucose levels, this pump has been used. Reignited the discussion over wearable security and whether manufacturers were taking enough measures to avoid such assaults after this on-stage demonstration [54]. Cyberattacks on the healthcare industry are a top priority, according to SANS' healthcare cyber threat study. Figure 2 demonstrates that 72% of healthcare facilities have been hacked by medical device vendors.

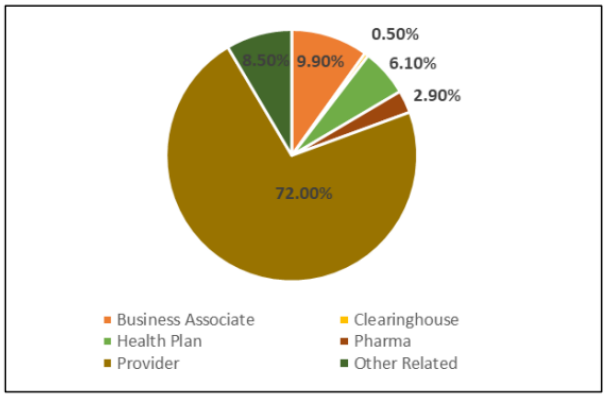


Figure 2: Organizations in healthcare compromised.

There were 65 healthcare establishments in the United Kingdom affected by the WannaCry ransomware in May 2018 [55]. Even MRI equipment were compromised by this cyber-attack.

Concerns about the safety and privacy of medical devices connected to the internet: Wearables capture an average of 310 MB of Physician Health Data (PGHD) per person every year. The yearly cost for thousand inhabitants is 31 TB [56]. The volume of patient information would only grow as wearable technology becomes more commonplace in healthcare. This study focuses on the security and privacy issues of wearable activity trackers. In light of the significance of security and privacy in the internet-connected devices, more sensitive content should be categorized, handled and secured with priority." The following diagram illustrates the internet's transmission of privacy-related information via user data. Automation is a common feature of most wearable gadgets. The convenience of computerized data is counterbalanced by the security risks it entails.

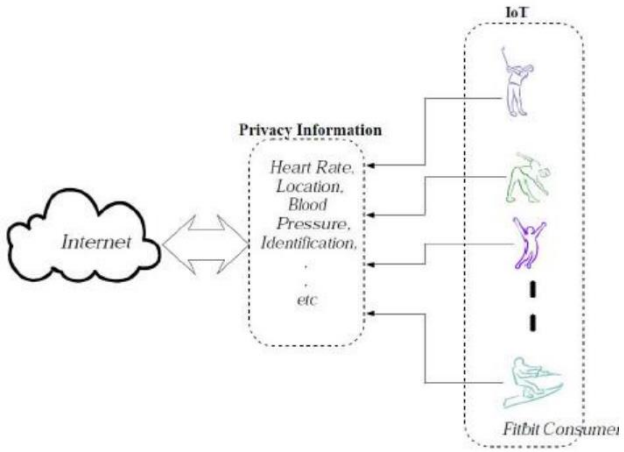


Figure 3: IOT and the security and privacy issue

We may now better grasp the structure of biosensor wearable devices thanks to Yan Wand and Yu work to highlight the drawbacks of existing wearable systems, this article also investigated several system implementations. In Figure 4, a smart healthcare system is shown. Patient data is gathered by the device's biosensors, and the information from across all sensors is relayed towards the Central Node through wireless or cable connectivity. In the Central Node, a CPU processes all the acquired data before it is distributed wirelessly to other applications.

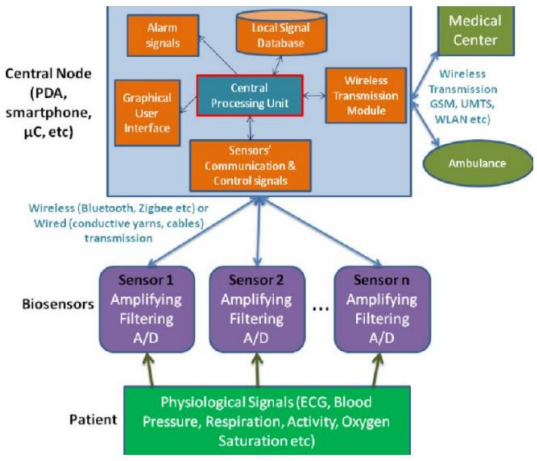


Figure 4: Architecture of a wearable health monitoring system

Wearable healthcare monitoring was discussed in detail; however, the authors did not provide any guidance on how to secure these devices. The privacy and security of medical

devices connected through the wrist-worn internet have yet to be studied from a stakeholder viewpoint to the best of my knowledge. All the publications in this part have helped me to better grasp the architectural style, communication methods, and security concerns of all these devices.

3. RESEARCH METHODOLOGY

Researchers hope that these findings may help users who are unsure about which wearable internet-connected medical device (IOMT) to choose, spur more healthy competition among IOMT device makers, and ultimately enhance the overall security of such devices for the general population. The MCDM (Multiple Criteria Decision Making) technique was used in this investigation. It's a decision-making method that takes into consideration a variety of factors, even those that clash. As a result, the goal of this article is to examine the current state of medical device security from the viewpoint of stakeholders.

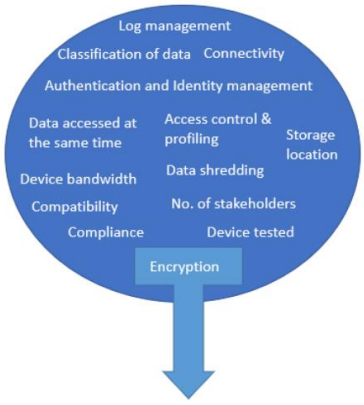
4. DATA ANALYSIS

IOMT device stakeholders may benefit from this paper's technique. Each stakeholder has a unique experience with the item. All stakeholders aren't necessary to have all of these criteria. The stakeholder-centric strategy helps stakeholders with a wide range of demands, objectives, and risk-tolerance preferences. Stakeholders within those devices include everyone from patients and physicians to hospitals and nurses to manufacturers and security experts.

This is a two-step process.

STEP 1: A questionnaire on the attributes of the smart wearable devices was completed. Device specs and privacy rules were considered while coming up with the answers to these queries.

STEP 2: As a result of this analysis, each attribute's score is calculated. It was determined that each attribute's score should be rounded up to a total of 10.



Does the device allow the user to select the data for encryption?
Does the device encrypt the passwords?
Does the device encrypt the data that is at rest?
Does the device encrypt the data in transit?
Does the device encrypt the data that is in use?
Does the device follow any of the standard encryption techniques?
If yes, Does the device comply with regulations in the country where it is used?
Does the device allow the user to choose an encryption technique?

Figure 5: Attributes and considerations.

Encryption is a key issue for medical wearable IoT devices, as shown in Figure 5, which shows the features needed to provide privacy and security.

Data Analysis

The following algorithm has been used to standardize attribute scores.

$$Attribute\ score = \sum_{i=1}^{N} Consideration_i \ X \ \frac{10}{N}$$

N = number of considerations

Stakeholder-centered approach. In the preceding part, all the features and factors were clearly specified. A stakeholder-centered approach is described in this part of the proposed paradigm. There are many players in the smart internet of medical things: patients, physicians, clinics, caregivers, producers, security researchers, regulatory bodies, and insurance companies Not every stakeholder necessitates the inclusion of all the above characteristics. All stakeholders are given the traits that are relevant to their role in the project.

Table 1: Stakeholder-Centric Approach

Stakeholders	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Patient	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hospital			X			X			X					X
Doctor			X	X	X	X	X		X			X		X
Nurse				X		X			X					X
Manufacturer	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Regulatory authorities		X		X							X	X		X
Insurance			X	X	X					X		X		
Security Researchers		X	X	X	X	X	X	X			X			X

Keys:

1 – Authentication and Identity management
2 – Access control and profiling
3 – Storage location
4 – Encryption
5 – Compliance
6 – Connectivity
7 – Data Shredding
8 – Classification of data
9 – Data accessed at the same time
10 – Number of stakeholders
11 – Device bandwidth
12 – Device tested
13 – Log management
14 – Compatibility

5. DISCUSSIONS

Dexcom g5 as well as the MiniMed 530G Insulin Pump | Diabetes Pump System with Smart Guard Technology are examples of wearable medical devices (Zak. Huber, 2016). MiniMed 530G. It is only after answering all the questions that these two gadgets are appraised. An appendix with the results of the Dexcom g5 as well as MiniMed 530G evaluations can be found here.

In the second stage, when all the questions are answered, the rating for each characteristic is calculated according to its considerations. All the qualities' ratings are averaged together to get a total of 10.

/

$$Attribute\ score = \sum_{i=1}^{N} Consideration_i\ X\ \frac{10}{N}$$

N = number of considerations

For better visualization, all attribute scores have been plotted in a graph. Figure 6 depicts a graph of all the attribute scores for the Dexcom G5 as well as MiniMed 530G.

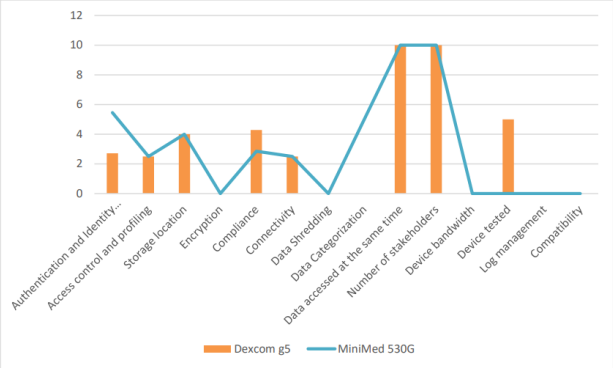


Figure 6: Comparison of two wearable IOMT devices.

Stakeholder-centered approach. Every stakeholder has its own set of needs, objectives, and level of comfort with taking risks. Therefore, the value of the gadget varies depending on who is using it. The graph below shows how it changes depending on who is involved. Figure 7 displays the Dexcom g5's values from the perspectives of two stakeholders: a patient and a clinician. For a device called the MiniMed 530G, the values of two are shown in Figure 8.

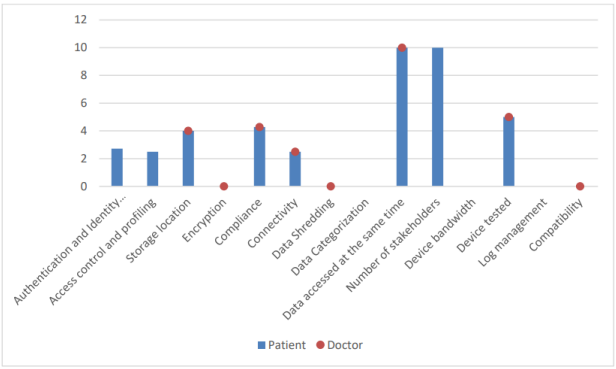


Figure 7: Comparison of a doctor and a patient for Dexcom g5.

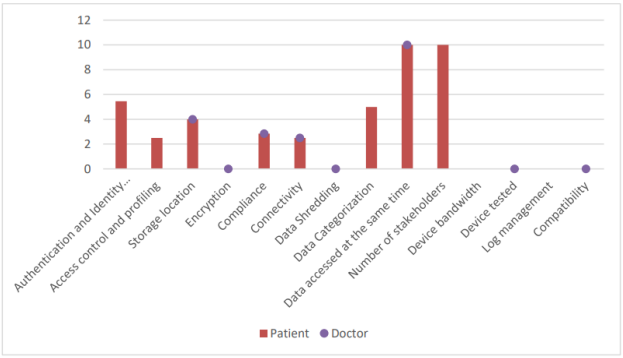


Figure 8: Comparison of a doctor and a patient for MiniMed 530G

6. CONCLUSION

A recent HIMSS poll found that two-thirds of healthcare firms had a major security incident. A lot of IoMT medical device researchers as well as manufacturers are concentrating on the S&P of all of these medical devices. As a result, several government authorities have taken major efforts to assure the protection of healthcare data and the compliance with medical equipment. Healthcare practitioners and patients who are interested in IoMT tend to focus on the device's performance and reliability rather than the security and privacy issues that come with these devices. Overlooking these security issues is most often due to a lack of knowledge.

Using this technique, IoMT users (such as physicians and nurses) may rate the protection and deterrent provided by wearable IoMT devices. A stakeholder-centric strategy is presented to enhance the security of wearables IoMT devices. Because it bases security on how users interact with wearable IoMT devices, this study is unique. A wide range of stakeholders, including those with differing requirements, objectives, and risk tolerance, may benefit from this strategy. This research has the potential to be developed to assist both device makers and end users. Wearable IOMT devices may be evaluated using this technique, resulting in an easy-to-use tool for doing so. The values of previously examined devices may be saved in this tool and retrieved by consumers. Each feature may be given a certain weight depending on the requirements of the various stakeholders.

REFERENCES

[1] H. M. Alzoubi, J. R. Hanaysha, M. E. Al-Shaikh, and S. Joghee, “Impact of Innovation Capabilities on Business Sustainability in Small and Medium Enterprises,” *FIIB Bus. Rev.*, vol. 11, no. 1, pp. 67–78, 2022, doi: 10.1177/23197145211042232.

[2] C. Mejia, K. Ciarlante, and K. Chheda, “A wearable technology solution and research agenda for housekeeper safety and health,” *Int. J. Contemp. Hosp. Manag. pp*, pp. 1–3, 2019.

[3] H. M. Alzoubi, H. Elrehail, J. R. Hanaysha, A. Al-Gasaymeh, and R. Al-Adaileh, “The Role of Supply Chain Integration and Agile Practices in Improving Lead Time During the COVID-19

Crisis," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 13, no. 1, pp. 1–11, 2022, doi: 10.4018/IJSSMET.290348.

[4] H. M. Alzoubi and R. Yanamandra, "Empirical Investigation of Mediating Role of Six Sigma Approach in Rationalizing the COQ in Service Organizations," *Oper. Supply Chain Manag. An Int. J.*, vol. 15, no. 1, pp. 2579–9363, 2022.

[5] T. M. Ghazal *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, 2022, doi: 10.1049/cmu2.12301.

[6] H. M. Alzoubi, M. In'airat, and G. Ahmed, "Investigating the impact of total quality management practices and Six Sigma processes to enhance the quality and reduce the cost of quality: the case of Dubai," *Int. J. Bus. Excell.*, vol. 27, no. 1, pp. 94–109, 2022, doi: 10.1504/IJBEX.2022.123036.

[7] S. Akhtar, A., Bakhtawar, B., & Akhtar, "EXTREME PROGRAMMING VS SCRUM: A COMPARISON OF AGILE MODELS Asma Akhtar, Birra Bakhtawar, Samia Akhtar," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 80–96, 2022.

[8] N. Nanayakkara, M. Halgamuge, and A. Syed, "Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review," 2019.

[9] B. Amrani, A. Z., Urquia, I., & Vallespir, "INDUSTRY 4.0 TECHNOLOGIES AND LEAN PRODUCTION COMBINATION: A STRATEGIC METHODOLOGY BASED ON LINKS QUANTIFICATION Anne Zouggar Amrani, Ilse Urquia Ortega, and Bruno Vallespir," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 33–51, 2022.

[10] T. M. Ghazal *et al.*, "AI-Based Prediction of Capital Structure: Performance Comparison of ANN SVM and LR Models," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–13, 2022, doi: 10.1155/2022/8334927.

[11] Nasim, S. F., M. R. Ali, and U. Kulsoom, "Artificial Intelligence Incidents & Ethics A Narrative Review. International Journal of Technology, Innovation and Management," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 2, pp. 52–64, 2022.

[12] H. M. Alzoubi *et al.*, "Empirical linkages between ICT, tourism, and trade towards sustainable environment: evidence from BRICS countries," 2022, doi: 10.1080/1331677X.2022.2127417.

[13] P. S. Ghosh, S., & Aithal, "BEHAVIOUR OF INVESTMENT RETURNS IN THE

DISINVESTMENT," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 65–79, 2022.

[14] S. R. Guntur, R. R. Gorrepati, and V. R. Dirisala, "Internet of Medical Things," *Med. Big Data Internet Med. Things*, vol. 4, no. 6, pp. 271–297, 2018, doi: 10.1201/9781351030380-11.

[15] H. M. Alzoubi *et al.*, "Fusion-based supply chain collaboration using machine learning techniques," *Intell. Autom. Soft Comput.*, vol. 31, no. 3, pp. 1671–1687, 2022, doi: 10.32604/IASC.2022.019892.

[16] S. Goria, "A DECK OF CARDS TO HELP TRACK DESIGN TRENDS TO ASSIST THE," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 1–17, 2022.

[17] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, "A Mobile Cloud based IoMT Framework for Automated Health Assessment and Management," *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, pp. 6517–6520, 2019, doi: 10.1109/EMBC.2019.8856631.

[18] F. Del and G. Solfa, "IMPACTS OF CYBER SECURITY AND SUPPLY CHAIN RISK ON DIGITAL OPERATIONS: EVIDENCE FROM THE UAE PHARMACEUTICAL INDUSTRY Federico Del Giorgio Solfa," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 18–32, 2022.

[19] H. M. Alzoubi, J. Hanaysha, and M. Al-Shaikh, "Importance of Marketing Mix Elements in Determining Consumer Purchase Decision in the Retail Market," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 12, pp. 56–72, 2021, doi: 10.4018/IJSSMET.2021110104.

[20] Saad Masood Butt, "Management and Treatment of Type 2 Diabetes," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.71.

[21] K. F. Cheung, M. G. H. Bell, and J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 146, no. July 2020, p. 102217, 2021, doi: 10.1016/j.tre.2020.102217.

[22] Edward Probir Mondol, "the Role of Vr Games To Minimize the Obesity of Video Gamers," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.70.

[23] H. M. Alzoubi and R. Aziz, "Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation," *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 2, p. 130, 2021, doi: 10.3390/joitmc7020130.

[24] Neyara Radwan, "the Internet'S Role in Undermining the Credibility of the Healthcare

Industry," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.74.

[25] H. M. Alzoubi *et al.*, "Securing Smart Cities Using Blockchain Technology," in *2022 1st International Conference on AI in Cybersecurity (ICAIC*, 2022, pp. 1–4. doi: 10.1109/icaic53980.2022.9896971.

[26] Nada Ratkovic, "Improving Home Security Using Blockchain," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.72.

[27] M. El Khatib, A. Al Mulla, and W. Al Ketbi, "The Role of Blockchain in E-Governance and Decision-Making in Project and Program Management," *Adv. Internet Things*, vol. 12, no. 03, pp. 88–109, 2022, doi: 10.4236/ait.2022.123006.

[28] Maged Farouk, "Studying Human Robot Interaction and Its Characteristics," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.73.

[29] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 382–391, 2019, doi: 10.1016/j.future.2019.01.008.

[30] N. Alsharari, "the Implementation of Enterprise Resource Planning (Erp) in the United Arab Emirates: a Case of Musanada Corporation," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.57.

[31] H. M. Alzoubi, A. U. Rehman, R. M. Saleem, Z. Shafi, M. Imran, and M. Pradhan, "Analysis of Income on the Basis of Occupation using Data Mining," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–4. doi: 10.1109/ICBATS54253.2022.9759040.

[32] Asem Alzoubi, "Machine Learning for Intelligent Energy Consumption in Smart Homes," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.75.

[33] H. M. Alzoubi *et al.*, "Digital Transformation and SMART-The Analytics factor," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–11. doi: 10.1109/ICBATS54253.2022.9759084.

[34] G. Ahmed and Nabeel Al Amiri, "the Transformational Leadership of the Founding Leaders of the United Arab Emirates: Sheikh Zayed Bin Sultan Al Nahyan and Sheikh Rashid Bin Saeed Al Maktoum," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.58.

[35] H. M. Alzoubi and R. Yanamandra, "Investigating the mediating role of Information Sharing Strategy on Agile Supply Chain in Supply Chain Performance," *Uncertain Supply Chain Manag.*, vol. 8, no. 2, pp. 273–284, 2020.

[36] G. M. Qasaimeh and H. E. Jaradeh, "The Impact of Artificial Intelligence on the effective applying of Cyber Governance in Jordanian Banks," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.

[37] H. Alzoubi and M. & Alnazer, N., Alnuaimi, "Analyzing the Appropriate Cognitive Styles and its effect on Strategic Innovation in Jordanian Universities," *Int. J. Bus. Excell.*, vol. 13, no. 1, pp. 127–140, 2017.

[38] John Kasem and Anwar Al-Gasaymeh, "a Cointegration Analysis for the Validity of Purchasing Power Parity: Evidence From Middle East Countries," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.60.

[39] H. M. Alzoubi, G. Ahmed, A. Al-Gasaymeh, and B. Al Kurdi, "Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration," *Manag. Sci. Lett.*, vol. 10, no. 3, pp. 703–708, 2020, doi: 10.5267/j.msl.2019.9.008.

[40] T. Eli and Lalla Aisha Sidi Hamou, "Investigating the Factors That Influence Students` Choice of English Studies As a Major: the Case of University of Nouakchott Al Aasriya, Mauritania," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.62.

[41] A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, vol. 174, no. May 2020, p. 102886, 2021, doi: 10.1016/j.jnca.2020.102886.

[42] H. M. Alzoubi, M. Alnuaimi, D. Ajelat, and A. A. Alzoubi, "Towards intelligent organisations: An empirical investigation of learning orientation's role in technical innovation," *Int. J. Innov. Learn.*, vol. 29, no. 2, pp. 207–221, 2021.

[43] D. Miller, "The Best Practice of Teach Computer Science Students to Use Paper Prototyping," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 42–63, 2021, doi: 10.54489/ijtim.v1i2.17.

[44] H. Alzoubi and G. Ahmed, "Do TQM practices improve organisational success? A case study of electronics industry in the UAE," *Int. J. Econ. Bus. Res.*, vol. 17, no. 4, pp. 459–472, 2019, doi: 10.1504/IJEBR.2019.099975.

[45] T. Eli, "Students` Perspectives on the Use of Innovative and Interactive Teaching Methods at the University of Nouakchott Al Aasriya, Mauritania: English Department as a Case Study," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 90–104, 2021, doi: 10.54489/ijtim.v1i2.21.

[46] H. M. Alzoubi, S. Joghee, and A. R. Dubey, "Decisions effectiveness of FDI investment biases at real estate industry: Empirical evidence from Dubai smart city projects," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 3499–3503, 2020.

[47] T. Mehmood, "Does Information Technology Competencies and Fleet Management Practices lead to Effective Service Delivery?," *Empir. Evid. from E-Commerce Ind.*, vol. 1, no. 2, pp. 14–41, 2021.

[48] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, 2021, doi: 10.1007/s11227-020-03570-x.

[49] S. A. Fatima, N. Hussain, A. Balouch, I. Rustam, M. Saleem, and M. Asif, "IoT enabled Smart Monitoring of Coronavirus empowered with Fuzzy Inference System," *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 6, no. 1, pp. 188–194, 2020.

[50] N. Alsharari, "Integrating Blockchain Technology with Internet of things to Efficiency," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 01–13, 2021, doi: 10.54489/ijtim.v1i2.25.

[51] H. M. Alzoubi, M. Vij, A. Vij, and J. R. Hanaysha, "What leads guests to satisfaction and loyalty in UAE five-star hotels? AHP analysis to service quality dimensions," *Enlightening Tour.*, vol. 11, no. 1, pp. 102–135, 2021.

[52] A. Akhtar, S. Akhtar, B. Bakhtawar, A. A. Kashif, N. Aziz, and M. S. Javeid, "COVID-19 Detection from CBC using Machine Learning Techniques," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 65–78, 2021, doi: 10.54489/ijtim.v1i2.22.

[53] H. M. Alzoubi *et al.*, "Modelling supply chain information collaboration empowered with machine learning technique," *Intell. Autom. Soft Comput.*, vol. 30, no. 1, pp. 243–257, 2021, doi: 10.32604/iasc.2021.018983.

[54] Vorobeva Victoria, "Impact of Process Visibility and Work Stress To Improve Service Quality: Empirical Evidence From Dubai Retail Industry," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.59.

[55] A. A. Kashif, B. Bakhtawar, A. Akhtar, S. Akhtar, N. Aziz, and M. S. Javeid, "Treatment Response Prediction in Hepatitis C Patients using Machine Learning Techniques," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 79–89, 2021, doi: 10.54489/ijtim.v1i2.24.

[56] H. M. Alzoubi, A. Ali, A. W. Septyanto, I. Chaudhary, H. A. Hamadi, and Z. F. Khan, "Applied Artificial Intelligence as Event Horizon Of Cyber Security," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS*, 2022, pp. 1–7. doi: 10.1109/ICBATS54253.2022.9759076.